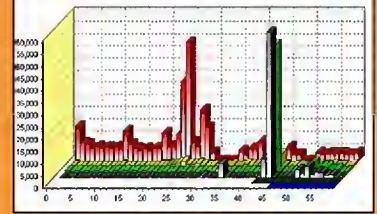


تقرير كامل حول دراسة الشبكات في الهند



تقرأون في هذا العدد

كيف يعمل بروتوكول SNMP



عشرة أوامر يجب أن تعرفها عن سيسكو

أهم الاختلافات بين ويندوز 2003 وويندوز 2008

ماهو بروتوكول UDLD وكيف يعمل

أداة Yarsinia الأفضل في اكتشاف ثغرات السويتش

والعديد من المواضيع الجديدة والقيمة

شاهدوا أيضا أقسام

مصطلحات تقنية

عتاد ومعلومات

مشاكل وحلول

نتائج الاستفتاء

ماهو أنطباعك حول دراسة الشبكات في الهند؟

تعتمد على مكان وأسم المعهد

62% ☐

ممتازة

24% ☐

سيئة جدا

5% ☐

جيدة

4% ☐

- رخص شديد
- سرعة كبيرة في التدريس
- توفير لابات وأجهزة حقيقية للعمل



كيفية أسترجاع كلمة السر
لأجهزة جونيبر

JUNOS
SOFTWARE

3



أفتتاحية العدد

نظرية التميز

أحد الأخطاء الشائعة التي نواجهها نحن كعرب هي عدم وجود أشخاص متميزين في مجالات محددة وخصوصا في مجال الكمبيوتر. فعندما أقول عن نفسي أنني محترف في الكمبيوتر أو في الشبكات فهذا لا يعني أي شيء لأحد لأن الكمبيوتر أو الشبكات تملك عالم كبير جدا لا يمكن اختصاره بكلمة محترف وتجد بعض الأشخاص عامل فيها محترف بتاع كله على قوله أخواننا المصريين يعني يفهم في سيسكو ومايكروسوفت وبيعرف في السكويرتي والفويس والبرمجة وخبرة معقولة في التصميم وبركب دشات وبيغسل سيارات وهذا كله على شان يلاقي وظيفة محترمة يستطيع من خلالها أن يحقق هدفه السامي وهو أن يتجاوز ويخلف ويعيش مستور والتي تسمى بنظرية التفكير المحدود والتي تنتهي بحصوله على الوظيفة .

وفي كل مرة أثير هذا الموضوع أجد الكثير من الأشخاص يدعي بأنني لا أعرف الواقع وأن الواقع يتطلب مني أن أكون ملم بكل هذه الأشياء وكلمة الواقع تعني أصحاب العمل الذين يقع عليهم العاتق الأول الذي يمنع شبابنا وجيلنا الصاعد في التفكير بأن يكون متميزا في أحد المجالات ومن هنا أحب أن أخطب أصحاب العمل بضرورة البحث عن الأشخاص المتميزين والذين قادرون على التطوير والانتاج بشكل أفضل وليس الأشخاص الذين يستطيعون أن ينفذوا كل ماتطلبونه وأعلموا أن هذه الأشياء سوف تحاسبون عليها يوم القيامة فأنتم أحد أسباب عدم تطور المجتمع العربي المسلم وأضيف على ذلك الاستفادة من التجارب الغربية في هذا المضمار والتي دانما كانت السند الأكبر لكل الأشخاص المتميزين أما السبب الثاني وهو الأهم هو أنت أخي العزيز لأن لو كان تفكيرك محدود فانت لن تصل إلى التميز وسوف تبقى دانما في أسفل القائمة فانت بعيون الجميع مثقف تعرف شيء من كل شيء وليس كمثل العالم الذي يعرف كل شيء عن شيء ولو قارنت بين الكلمتين لوجدت أن العالم أثقل بكثير من المثقف ولو فكرت فيها بشكل صحيح لوجدت أن فكرة التميز هي التي سوف تجذب الوظيفة لك وليس العكس وأنسى أن هناك كلمة تدعى أحباط في حياتك لأن التميز والأحباط لايتفقان وإذا كنت تعتقد بأنني أتفلسف عليك فلا داعي لأن تستكمل قراءة المقال. وسبب دعوة إلى التميز يعود إلى سبب واحد وهو أن آوان النهضة العربية يجب أن يبدأ نحن لانريد الانتاج الآن لكن نريد منك أن تفكر كيف نبدأ الانتاج؟ هل ياترى فكر أحدا ما منكم كيف تم كتابة البروتوكولات التي تعمل في الشبكات؟ بأي لغة كيف أستطيع أن أطورها؟ هل خطر على بالك أن تبحث عن المشاكل التي سوف تواجه بروتوكول IPv6 في المستقبل وحاول أن يفكر في بعض الحلول؟ الأسئلة كثيرة أخي العزيز وأعلم أنه لا يوجد شيء كامل وكل شيء قابل للتطوير والزيادة وهو ماأطلبه منك في الوقت الحالي أن تبدأ دراسة الأساسات والتي سوف تفتح لك أبواب التطوير والأرتقاء بعالمنا العربي المتردي وأكتب قول الله تعالى على جبينك "إن الله لا يضيع أجر من أحسن عملا" ولكل مجتهد نصيب في الدنيا وأعلم أيضا أن الرزق على الله وأنتك سوف تصل يوما ما إلى أعلى المراتب ودمتم بود أيمن النعيمي

المحررون الدائمون

- الدكتور محمد التميمي

Yarra_link@yahoo.com

- المهندس أيمن النعيمي

www.networkset.net

- المهندس أحمد الشحات

warior10@hotmail.com

- المهندس عادل الحميدي

adel_husni2000@hotmail.com

- المهندس ياسر رمزي

www.yasserauda.com

موقع المجلة

www.networkset.net

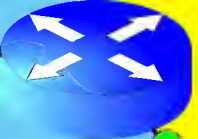
بريد المجلة

magazine@networkset.net

بريدي الخاص

admin@networkset.net

جميع الحقوق محفوظة لكاتبها



محتويات حزينان 2110



تقرير كامل عن دراسة الشبكات في الهند (الصفحة رقم 5

- | | | |
|----|---|---|
| 15 | 3 - كل ماتحتاج أن تعرفه حول بروتوكول الـ SNMP | - من أين وكيف أبدأ طريق الشبكات |
| 16 | 4 - ماهي تقنية الـ Auto-MDIX | - ماهو بروتوكول الـ UDLD ؟ وكيف يعمل ؟ |
| 16 | 8 - مقارنة بين منفذي الـ Console و Aux | - إصدار جديد من برنامج البايت ترايسير |
| 17 | 8 - كيف تقوم بتأسيس شبكة فويس من الصفر | - إصدار جديد من برنامج الـ GNS3 |
| | 9 قسم الأمن والحماية | - كيفية استعادة كلمة السر لاجمزة جونيبر |
| 19 | 10 - هجوم stp manipulation وطريقة التصدي له | - أربعون سنة تمر على الانترنت |
| 20 | 11 - Yarsinia لاكتشاف الثغرات الموجودة في السويتش | - نتائج الاستفتاء الشهري |
| 21 | 12 قسم عتاد ومعلومات | - عشرة أوامر يجب أن يعرفها كل شخص يتعامل مع سيسكو |
| 23 | 13 قسم مصطلحات تقنية | - كيفية أسترجاع كلمة السر الخاصة بالدومين (AD) |
| 24 | 14 قسم مشاكل وحلول | - أهم الاختلافات بين ويندوز 2003 و ويندوز 2008 |



من أين أبدأ وكيف أبدأ في الشبكات؟؟؟

سؤال لطالما حيرني!!!

بقلم: عادل الحميدي



وخصوصاً أن هذا المنتدى وغيره به عدد لا يستهان به من المهندسين العرب المتخصصين والمميزين والمحترفين حقيقة في هذا المجال ، ولعل المقام هنا مناسب لأوجه لهم نداء لبذل مجهود أكبر في خدمة هذه الأمة بمزيد من الشروحات والنصائح والمقالات والتي لا يستغنى عنها أحد ، كما نقول لهم جزاكم الله خيراً على ما قدمتموه لنا من علم حتى الآن وننتظر المزيد أمتكم في حاجة ماسة إليكم .

لكن إذا كانت هناك مشكلة حقيقية فستكون في اللغة الإنجليزية لأن معظم هذه المواد التعليمية المساعدة باللغة الإنجليزية فإن كانت لديك اللغة الإنجليزية جيدة ستجعلك تنطلق في هذا المضمار بشكل أسرع .



يأتي أحدهم ويقول لي ألم أقل لك لن أستطيع لأني ضعيف في اللغة الإنجليزية ، هذا غير أن كورسات اللغة أيضاً مكلفة ؟ يا أخي الكريم أنا عهدتك أعلى همة من ذلك ، وإليك النصائح التالية في اللغة الإنجليزية

تعلم اللغة أمر بسيط جداً ومشكلة حلها بسيط جداً ... بداية كل شيء تكون غير سهلة (لاحظ لم أقل صعبة) وكما يقولون "مفيش حلاوة من غير نار ، ومفيش ورد من غير شوك" ، مشكلتنا الحقيقية في اللغة أننا نحفظ كلمات وليس جمل ، ولعل هذه مشكلة يطول شرحها ولكني سأحيلك على أفضل موقع لتعلم اللغة وقعت عليه عيني استفدت منه حقيقة كثيراً واشترت منه كورس

<http://learnreallenglish.com/>

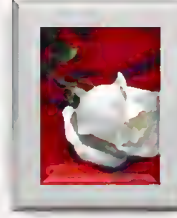
ولعلي أرفعه لكم وأعطيتكم الرابط في العدد القادم أسألكم الدعاء ، وهذا الموقع له طريقة جديدة جداً في تعلم اللغة ، وهذه الطريقة "أتت على الجرح" كما يقولون ، تعلمك كأنك طفل صغير ، لن أطيل عليكم وإن شاء الله أرفع الكورس لكم بقواعده السبعة التي بنيت عليها فكرة التعلم الجديدة هذه ...

لكن لا تنتظر أبداً ويمكنك أن تستخدم جوجل للترجمة (جوجل ذلك الموقع العبقري) ، فأني كلمة لا تعرفها إبحث عن معناها يمكنك أيضاً كتابة الجملة كاملة وجوجل للترجمة يترجمها لك ، دعني أخرجك من حالة الجد هذه بموقف طريف حدث لي أنا شخصياً ...

كنت في " سنة أولى جامعة " وكان عندنا مادة حاسب آلي باللغة الإنجليزية ، وجلست ليلة كاملة أترجم في صفحة لمدة خمس ساعات وبعدها إكتشفت أنها مقدمة الكاتب !!! لكنني تعلمت

لكن تياس وتقول صعب لن أستطيع ، فهذا كلام فارغ معناه إنسان فاشل ، ليس لديه طموح وهمة ، أرجوكم سامحني على هذه الكلمات لكن أرجوكم إمسح هذه الكلمات من قاموسك ، وأعلم أنك إن أخذت بالأسباب فإله سيسر لك أمرك ، فلا تياس من روح الله... والآن أريد أن أجيب عن تساؤل هام كثيراً ما يطرح وهو ... هل أستطيع الآن أن أعمل في مجال الـ IT ؟ وخصوصاً بعد حصولي على شهادتي +A ، +N ،؟؟؟

والإجابة هي نعم تستطيع وبكل تأكيد فأنت الآن خطوات أولى خطوات التميز ، أعرف أنك الآن فرح بما أقول ، لكن دعني أنبهك لشيء هام وهو : إن تحصيل فرصة العمل تلك قد يكون صعب بعض الشيء ، وخصوصاً في مجتمع عربي مليء بالواسطة وغيرها من الأمور التي تحيل دون وصول المميزين لما يستحقون لكن لا تجعل ذلك يشطبك فأبحث وأعلم أن الله لن يخيب سعيك ولن يضيع تعبك " إن الله لا يضيع أجر من أحسن عملاً " .



لا أعرف كيف أبدأ لكن افتقدكم خلال هذا الشهر ، والذي مر علي بشكل صعب وخصوصاً من الاستفسارات التي وصلتني على الإيميل والتي بعضها كان محرراً ... كما أنها كانت كثيرة بشكل لم أتوقعه والحمد لله .

أصعب سؤال وصلني حقيقة كان : ماذا حققت أنت من هذه الخطة التي ستضعها ؟؟؟

دعني أجيب وعلى الملأ كما يقولون ، بفضل الله يا إخواني وأقولها بملء فمي بفضل الله وحده حققت 90% منها

فإذا لم يكن عون الله مع الفتى *** فأول ما يقضي عليه اجتهاده

فأنا في خلال ثلاث سنوات ونصف حصلت على كل الكورسات التي سأتكم عنها في خطتنا ولا تنسوا شعار هذه الخطة " مهندس شبكات محترف في ثلاث سنوات "

أعرف أن البعض قد يقول لي لكن المدة زادت عن ثلاث سنوات ، ولماذا تقول 90% مع أنك تقول حصلت على كل الكورسات التي ستتكلم عنها ، دعني أزيدك من الشعر بيتاً ، بل ستتعجب إن قلت لك أنني لم أختبر وأحصل على شهادة الـ A+ إلا من أسبوع وكان محفزي لهذا - سؤال محرج كما قلت لكم من أحد المبتدئين ، حيث أنني درست لها لكن لم أختبرها لظروف مادية ، وهذا لكي تعلم أنك لست وحدك تعاني من ظروف أصعب منك لكن لا تستسلم واستعن بالله ولا تعجز .

وإجابتي عن هذه الاعتراضات كالتالي : هي أنني لما قلت لكم في المقالة السابقة " ما كتبت هذا الكلام إلا بعد عناء طويل أخذ من عمري سنين بل أستطيع أن أقول أنني رويت بداية هذا الطريق بدمي " كنت أعني أن هذا المخطط نشأ من الخبرة والتي تعبت فيها فلا أريد لأحبابي في الله أن يتعبوا بل عليهم أن يتعلموا ممن سبقهم ، وأحفزكم أكثر فأنا والله الذي لا إله غير أحبك في الله وأتمنى ألا تعانوا كما عانيت أنا ، والله هذه الخطة إن سرتم عليها لن تستغرق منكم أكثر من سنتين صدقوني ، وأبدأ يا من تسأل كيف أبداً ؟ وكفاك تأخر والآن المقالة الثانية ...

توصلنا إلى أننا سنبدأ بكورس A+ ثم N+ وتلك هي البداية الصحيحة في طريق الامتياز والاحتراف ، دعنا نفترض أن كورس A+ سيسغرق ثلاثة أشهر و N+ ثلاثة أشهر ، والغرض الآن من تحديد المدة هي ربط الكورسات بالمدة السنوات الثلاث ، يعني الآن طرحنا 6 شهور من المدة الزمنية ، وعلى فكرة سيأتي عليك بعد ذلك كورسات أصعب من A+ و N+ وستنتهي في وقت أقل والسبب في ذلك أن البداية فقط تكون غير سهلة (لاحظ لم أقل صعبة) ، فلا تستكثر المدة فكم ضاع من أعمارنا في ما لا ينفع بل ما يضر والله المستعان (حاسبوا أنفسكم قبل أن تحاسبوا) ... ولعل هذا هو السبب وراء أنني زدت مدة هذه الكورسات عن الطبيعي بعض الشيء لرعاية حال المبتدئين ، حيث أنها تستغرق أقل من ثلاثة أشهر .



بعضهم يقول لي هذا ما كنت أخشاه ، المدة الزمنية " وقلنا ماشي " لكن ... التكلفة المادية لهذه الكورسات نحن في البداية وفي أول كورسين فقط ، هل تعرف إن تكلفتهم عندي في بلدي كذا وكذا ...

مبلغ كبير كيف ساكمل المشوار " والحالة تعبانة" كما يقولون ؟

أولاً : أعتذر عن إيراد مثل هذه الإشكالات والتي تطيل المقال لكنني مضطر فعلاً حيث أحاول أن أجيب في مقالاتي هذه عن كل الاستفسارات والتي تأتيني على الإيميل ، وأرجو أن تلاحظوا أن المقالة للمبتدئين الحياري والتائهين ... وإن لم أجيب فما حققت هدف هذه السلسلة .

ثانياً : الإجابة أن الإنترنت مكتبة مليئة بالمواد التعليمية المساعدة على دراسة هذه الكورسات ، كما أن هذه المكتبة بها ملفات متنوعة فيديو وأكرويات وورد وبوربوينت ، ومنها ما هو باللغة العربية لكن أغلبه باللغة الإنجليزية ، ومن أشهر الأمثلة العربية على ذلك منتدى عرب هاردوير وبوابة العرب التعليمية و... ، ودعني أتفق مع المهندس / أيمن النعيمي عندما قال عن نتائج الإستفتاء عدد الشهر الماضي " أن منتديات عرب هاردوير قد حولت عالم الشبكات إلى تاريخان تاريخ الشبكات قبل عرب هاردوير وتاريخ الشبكات بعد عرب هاردوير " .

✓ Experience ✓

والآن بعد الإنتهاء من الكورسين A و N+ تستطيع الاختيار بين مسارين :
سيسكو :الأول ... CCNA -> CCNP -> CCIE
مايكروسوفت :الثاني ... MCP -> MCSA -> MCSE
إلى اللقاء في الحلقة القادمة #
تقرأون في هذه الحلقة ...
مهندس شبكات محترف في ثلاث سنوات
أسئلة المبتدئين وإجاباتها
كيف تحصل على الخبرة Experience
تقرأون في الحلقة القادمة ...
CCNA -> CCNP -> CCIE ... سيسكو

الأمر الثاني هو : أن معدل الرواتب في هذه المرحلة ضعيف بعض الشيء وقد يكون ضعيف جداً ، لكن إبدأ إبدأ إبدأ ، فمن الأشياء المهمة والتي تزيد من سرعتك في السوق وزيادة الطلب عليك هي الخبرة Experience ، ولن تستطيع الحصول على الخبرة إذا لم توافق على أن تستغل في هذه المرحلة وسامحني على هذا اللفظ ففعلاً أصحاب الأعمال سيستغلونك في هذه المرحلة بحجة أنهم يعلمونك وتأخذ خبرة ، لكن لا تدع الفرصة إن أنت تفوتك ...



وأعلم أن الله جل جلاله كان قادراً على أن يخلق الكون في كن فيكون فأمره بين الكاف والنون ، ولكنه سبحانه بحكمته خلق السماوات والأرضين في سبع أيام ، ليعلمنا الصبر وأن كل شيء باؤان ... فأنت لو سرت على تلك النصائح وبتوفيق الله ستكون في المقدمة ، ويصل راتبك إلى 60 ألف أو يزيد ، أعرف أنك قد لا تصدق مثل هذه الأرقام عندما تسمعها ، لكن الواقع والأرقام هي التي تتكلم فهذا له وجود في مجال ال IT والله الموفق ... في الحقيقة أعرف أنني أظلت عليكم لكن الله أسأل أن ينفعني وإياكم بهذه الكلمات والتي والله تخرج من القلب لعلها تصل إلى قلوبكم ...

ماهو بروتوكول ال UDLD وكيف

بقلم: أيمن النعيمي

يعمل ؟

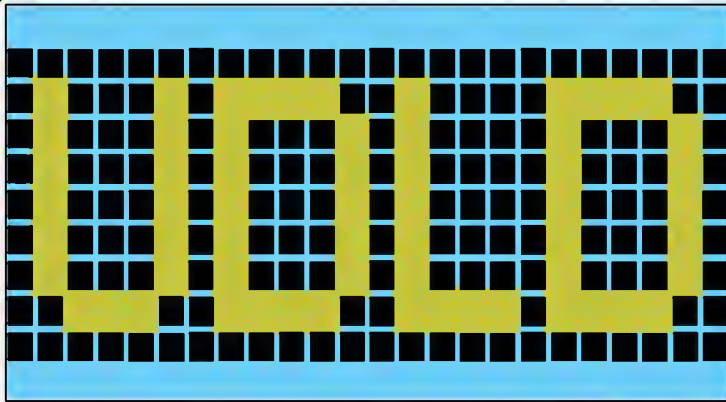
مقدمة

UDLD أو Unidirectional Link Detection هو أحد البروتوكولات التي قامت سيسكو بتطويره وهو يعمل في الطبقة الثانية ووظيفته إيجاد المشاكل التي من ممكن حدوثه على الطبقة الأولى Physical Layer من خلال مراقبة عمل المنافذ وبالتحديد مراقبة حالة الأرسال والاستقبال التي تتم على المنفذ نتكلم عن الموضوع بشكل أوضح

لنفرض أن لدينا سويتشان مرتبطان مع بعضهما البعض بأكثر من منفذ ولنفرض منفذان وطبعا في هذه الحالة سوف يعمل بروتوكول STP لكي يمنع اللوب بينهما من خلال وضع أحد المنافذ في حالة Blocking والتي تتم من خلال إرسال ال Root Bridge BPDUs إلى السويتش الآخر مخرجا إياه بوجوب وضع أحد المنافذ في حالة Blocking وحتى هذه اللحظة كل شيء واضح لكن لنفرض هذه الفرضية بأن البورت الذي تم إرسال الفريم إليه لم يستلم أي شيء والسبب هو وجود مشكلة في الكابل وتحديدًا في الطرف المسؤول عن عملية الاستقبال وطبعا أول شيء سوف يخطر على بالك هو كيف يمكن حدوث هذا الشيء ؟ والجواب هو أن هذه المشاكل تحدث عادة في أسلاك الفايبر ونادرا ما تحدث للأسلاك العادية المعروفة بي ال UTP لكن محتمله والتي سوف تسبب لي Loop بسبب عدم استلام أي BPDUs من أحد المنافذ الموجودة في السويتش الثاني وسوف تدخل الشبكة في مشكلة كبيرة والسبب هو Unidirectional Link أو لينك أحادي الاتجاه يا أما يستقبل يا أما يرسل وليس الأثنان مع بعضهما البعض يعني ممكن نجد اللينك يقوم بالأرسال فقط ولايقوم باستقبال أي شيء أو نجد العكس! وطبعا الناتج كارثي نوعا ما على الشبكة بسبب حدوث مشكلة على الطبقة الأولى أثرت في عمل بروتوكول يعمل على الطبقة الثانية والجدير ذكره أنك من خلال مراقبتك لحالة المنافذ لن تجد أي شيء يدل على أي شيء لذا سوف تكون المشكلة أكبر

كيف يعمل ال UDLD ؟

لنتفق أولا على ضرورة تفعيل البروتوكول على كلا الطرفين وتبدأ العملية من خلال استكشاف كل سويتش للآخر من خلال إرسال فريم خاصة بأجهزة سيسكو ممكن أن نطلق عليها Hello msg أو advertisement msg وترسل على العنوان التالي 01:00:0C:CC:CC:CC وهذا العنوان طبعا هو - MAC address Multi-cast وتحتوي هذه الفريم device ID مع port ID (يقوم البروتوكول بأبتكاره) بالإضافة إلى قيمة تحدد مدة بقاء الفريم محفوظة في السويتش الآخر نطلق عليها timeout وعندما تصل إلى الطرف الآخر تخزن في الذاكرة حتى تنتهي المدة التي أشرنا إليها وطبعا قبل أن تنتهي سوف يصل فريم جديد يحل مكان القديمة وبهذه الطريقة تبقى السويتشات في حالة مراقبة لكل البورتات المتصلة مع السويتش الآخر وإذا أحببت أن تستزيد أكثر عن الموضوع فأتجه إلى RFC5171 (ملاحظة هامة وهي أن الفريم يرسل من خلال كل المنافذ الموجودة بين السويتشان مع تغيير قيمة ال-POR (ID



ماهي ردة فعل ال UDLD في حال حدوث مشكلة في اللينك؟

تعتمد ردة الفعل على كيفية أعدادنا للبروتوكول على السويتش وهو بشكل عام يملك وضعيتان يمكن أعدادهم الوضعية الأولى Normal وفيها لن يقوم السويتش بإيقاف عمل البورت وسوف يستمر عمل البورت بشكل طبيعي وبدون تغيير حالة ال STP والشئ الوحيد الذي سوف يحدث هو إضافة كلمة undetermined إلى جانب المعلومات الخاصة بالبورت وبكلام آخر عندما تقوم بعرض حالة البورتات الموجودة من خلال الأمر Show ip inter-face brief سوف تلاحظ وجود كلمة undetermined بجانب أسم البورت والتي سوف تلفت نظر مسؤول الشبكة حول حدوث مشكلة في اللينك الوضعية الثانية هي Aggressive وهي تقوم مباشرة بتحويل البورت إلى errdisable أي تقوم بإيقاف البورت بشكل كامل وقبل أن يقوم بهذا العمل يقوم البروتوكول بأرسال 8 فريم كل ثانية حتى يتأكد أن البورت يواجه مشكلة فعلية وليست شيء عابر وبعدها يتم الأيقاف

طريقة الأعداد

كما أقول دائما أن طريقة الأعداد هي أسهل شيء في الموضوع وهي تتم من خلال التوجه إلى المنفذ وكتابة الأمر التالي

```
Switch(config-if)#udld port aggressive
```

إذا في حال أردنا أن يكون الوضع هو normal لانقوم بكتابة aggressive

ملاحظات هامة

يعد هذا البروتوكول كمساعد لل STP لأنه أكثر بروتوكول يمكن أن يتأثر بهذه المشكلة هو STP

هذا البروتوكول مدعوم في سويتشات Catalyst فقط

بعض السويتشات يدعم الوضعيتين والبعض الآخر يدعم وضعية normal فقط (سياسة خبيثة من سيسكو!) هذا رابط يوضح المودلات المدعومة - UDLD Availability on Catalyst switch

يمكننا تغيير قيمة ال Timeout في بعض المودلات من خلال الأمر udld interval 10 وهي قيمة تتراوح من 7 إلى 90 ثانية والقيمة الطبيعية هي 15

تقرير كامل عن دراسة الشبكات في الهند

أعداد: عبدالمجيد خالد الكثيري

الجامعة وتنتشر ضمن منطقة جغرافية محددة من قبل الحكومة الهندية وذلك حسب الصلاحية القانونية التي أعطيت للجامعة. وان أغلب هذه الكليات تطرح برامج البكالوريوس فقط، ما عدا البعض منها يطرح برامج الماجستير. وان اكبر أنواع هذه الجامعات هي: جامعة دلهي، وكلكتا، ومومباي وبنجلور حيث يتبع لكلا واحدة منهم المئات من الكليات.

* الجامعات الخاصة Deemed Universities

أن هذا النوع من الجامعات كانت بداية كل واحدة منها عبارة عن معهد خاص للتعليم العالي، ولكن أعطي مسمى الجامعة لمرور عدة سنوات على إنشائه وتميز برامجه وخرجيه. وبعدها أعطي مسمى جامعة خاصة Deemed University، حيث يمنح هذا النوع من الجامعات كذلك الدرجات العلمية المختلفة مثل البكالوريوس والماجستير والدكتوراة.

* المعاهد ذات الأهمية الوطنية Institutions of National Importance

هناك أحد عشر معهدا في مختلف الولايات الهندية حاصلة على الصلاحية الخاصة بإعطاء الدرجات العلمية المختلفة وذلك نظرا لتمييزهم (حيث انه حسب القانون الهندي لا يحق لأي جهة غير جامعية إعطاء الدرجات العلمية المختلفة). من بين هذه المعاهد هناك عدد 6 منهم يطلق عليهم مسمى المعاهد الهندية للتكنولوجيا Indian Institutes of Technology وعادة يكون الحصول على قبول في هذه المعاهد صعبا جدا حيث أن الإقبال عليها شديد وذلك نظرا لتمييزهم.

أنواع الكليات

هناك 4 أنواع من الكليات، وهم كآلاتي:-

* الكليات الحكومية Government Colleges

أن عدد هذه الكليات قليل حيث يشكل ما نسبته 15% إلى 20% من مجموع الكليات في جمهورية الهند. وان إدارتهم تكون من قبل حكومة الولايات. وان الحصول على مقاعد للدراسة فيهم بالنسبة للطلبة الأجانب يكون صعبا، إلا اذا كان الطالب قادم عن طريق أحد البرامج الرسمية المرتبطة باتفاقيات ثقافية مع جمهورية الهند.

* الكليات الخاصة Private Colleges

هذا النوع من الكليات يشكل حوالي 70% من مجموع الكليات في جمهورية الهند، حيث انهم قد انشؤوا من قبل جهات خاصة، عادة ما تكون على شكل جمعيات وشراكه بين أفراد وهذا يعرف بنظام ترست أو الجمعيات trusts or societies. وان علاقة هذه الكليات محددة من قبل التشريع الخاص بالولايات المحلية. وان معظم الكليات الخاصة تستلم معونات مالية من قبل حكومات الولايات.

* كليات الجامعات University Colleges

ان هذه الكليات تدار من قبل الجامعات أنفسها، وأن عدد هذا النوع من الكليات قليل جدا.

* الكليات المتخصصة Professional Colleges

أن أغلب هذه الكليات تكون في تخصصات الطب medicine والهندسة engineering والإدارة management. وبعضها يدار من قبل حكومات الولايات والبعض الآخر من قبل جهات خاصة. وان أعداد هذه الكليات الحرفية المتخصصة أخذ في الازدياد في كلا من ولاية كراتاكا ومهراشتر واندرا برائش وتميل نادوا. وان هذه الكليات لا تحصل على دعم مالي من حكومات الولايات، ولهذا فأن رسوم الدراسة في هذه الكليات تكون مرتفعة جدا، خاصة بالنسبة للطلبة الأجانب، أو الطلبة غير قاطني جمهورية الهند Non-Residential of India N.R.I، حتى ولو كانوا يحملون الجنسية الهندية ولكنهم لا يسكنون في

مقدمة عن الهند

منذ القرن الحادي عشر، أسس المسلمين مدارس ابتدائية وثانوية وكذلك كليات وجامعات في مناطق عديدة مثل دلهي وكنوا والله آباد. وفي أغلب الأحيان كانت اللغة العربية هي لغة التدريس. وعند وصول البريطانيين الى الهند في القرن الثامن عشر، فقد فتحت عدة كليات بواسطة المبشرين المسيحيين، ثم تتابع بشكل سريع فتح الجامعات العديدة حتى وصل الآن حسب الإحصائيات الجديدة إلى مايزيد عن 340 جامعة وكلية وكذلك معاهد تعليمية عليا في مستوى الجامعات في مختلف الاختصاصات والمراحل بمختلف مناطق جمهورية الهند والتي تعد شبه قارة..

ويوجد من تزواج من الانجليزي ويسمون بالانقلو انديان وهم افضل من يتحدث اللغة الانجليزي بطلاقة بعد بلد المنشأ الانجليزي وهم متواجدون لأعداد لا بأس به وكذلك في أغلب الأحيان يعتبرون انفسهم بانهم من طينة خاصة بحيث ان السكن معهم او طلب التعلم عندهم مكلف بعض الشيء..

لماذا الهند؟

أعتراف عالمي، لغة إنكليزية ابننا حليت وانا اتكلم هنا عن مدينة حديثة كبنقلور، سهولة وعدم تعقيد الدراسة، الرسوم المعيشية والدراسية مناسبة جدا للجميع، توفر كافة التخصصات والمراحل الدراسية والدورات التخصصية وبأسعار خيالية كمدينة حيدر اباد، اما من ناحية الحصول عالميا فتعتبر غير معقدة مقارنة ببعض الدول الاخرى مع حدوث تغييرات كبيرة بعد احداث مومي الاخيرة وسوف ادراج بعض النقاط المهمة في نهاية التقرير مع مقارنات بسيطة، واود ان اضيف نقطة وهو الوجود الكبير للجنالية الهندية في اغلب مجالات التقنية في كل مكان وهو التعليم الجيد ورضائه بالراتب الموجود وعدم الاشتراط لانه يعرف انه في بداية حياته وبعد اكتساب الخبرة تاتيه الوظائف تلو الاخرى وكذلك كثر تواجدهم في الخليج والدول الاوية وهو رخص اليد العاملة كمثال بسيط يوجد في بنقلور مدينتين اي تي للشركات الكبرى بحيث شركات مثل قوقل ومايكروسوفت لديها شركات كبيرة هنا بيد عاملة هندية حيث ان راتب العامل لا يكلفهم مثل مايكلفهم العامل الامريكي او الاوربي حيث يتم تقسيم راتب الامريكي الواحد لعدة اشخاص هنود بمقارنة بسيطة لو كان راتب الامريكي عشرة الاف دولار فالهندي يرضى بالف دولار واعرف اشخاص يستلمون هذا المقدار وموظفين في مايكروسوفت وتم تشغيل عشرة اشخاص بدلين للامريكي بنفس راتب الامريكي ولكن سوف ينجزون بكل تأكيد عمل اكبر وادق

أنوع الجامعات والكليات الموجودة في الهند

تنقسم الجامعات الهندية إلى أربعة أنواع رئيسية وهي:-

* النوع المركزي Unitary

حيث يقتصر هذا النوع من الجامعات على حرم جامعي واحد تطرح في تخصصات البكالوريوس وكذلك برامج الدراسات العليا (الماجستير والدكتوراه)، ويعطي أهمية خاصة للبحث العلمي. ومثالا على هذه الجامعات هم: Aligarh Muslim

University Banaras Hindu University

* النوع الذي له كليات تابعة Affiliating Colleges

هذا النوع من الجامعات هو السائد في شتى الولايات الهندية وهو يتمثل في أن للجامعة حرم جامعي واحد أو اكثر يضم كليات ودوائر تقدم برامج الدراسات العليا وتقوم بمهمة إجراء الأبحاث. وتكون هناك كليات عديدة خارج الحرم الجامعي تقدم برامج

جمهورية الهند حاليا، يدفعون نفس رسوم الطلبة الأجانب. وقد قامت مؤخرا المحكمة الهندية العليا **supreme court** بوضع ضوابط وقوانين فيما يختص بعملية الالتحاق بهذه الكليات والرسوم الدراسية.

وان مختلف هذه الكليات المذكورة أعلاه تتبع جميع أنظمة الجامعات التابعة لها، فيما يخص بتدريس المناهج الدراسية وكذلك الأمر بالنسبة للامتحانات وان الشهادات والدرجات العلمية تمنح من الجامعة فقط

اللغة المستخدمة في التدريس

اللغة الإنجليزية هي اللغة المستخدمة في التدريس في جميع التخصصات، وخاصة التخصصات العلمية والطب والهندسة وفي جميع برامج التعليم العالي، إلا انه قد تستخدم اللغات المحلية بجانب اللغة الإنجليزية أحيانا في التخصصات الإنسانية والاجتماعية والتجارية.

التعلم عن بعد Distance Education

يرجع تاريخ بدء التعلم عن بعد في الجامعات الهندية إلى عام 1962م. وفي عام 1982 تأسست الجامعة المفتوحة **Open University** في مدينة حيدر آباد وولاية أندرا برادش، ثم تلاها تأسيس جامعة انديرا غاندي الوطنية المفتوحة **Indira Gandhi National Open University** في دلهي. هذا وقد افتتحت عدة جامعات برامج التعلم عن بعد في مختلف الولايات الهندية وذلك من أجل خدمة الأفراد العاملين والراغبين في الدراسة. وللمزيد من التعرف على البرامج المتوفرة في وشروط القبول .. الخ في التعلم عن بعد، يمكن الإطلاع على إصدار اتحاد الجامعات الهندية الخاص بذلك والذي يحمل عنوان **Distance Education** وهو متوفر في مكتب المعلومات الجامعية وزارة التربية والتعليم.

قبول الطلبة الأجانب

أن جميع الجامعات الهندية من حيث المبدأ تقبل الطلبة الأجانب وان رسومهم تختلف عن رسوم الطلبة المواطنين الهنود وفي بعض الأحيان هي محددة من قبل المحاكم الهندية. وكذلك على الطلاب الأجانب ان يدفعو مبلغ معين كرسوم تسجيل او كعطية من الطالب للكلية او الجامعة عند بداية التسجيل وتختلف من جامعة لآخر في مقدارها

الحصول على القبول من المعهد او الجامعة

طبعاً من المتعارف عليه ان من سيأتي للهند سوف يكون عن طريق زميل او قريب سبق له الدراسة فالهند وعن طريقه يتم طلب ورقة القبول وهم اعرف بها بحيث تطلب منه ورقة قبول من معهد لغة

او جامعة اذا اراد اكمال الدراسات العليا ولكن الاغلبية فالبدء ياتون لدراسة اللغة ويوجد نوعين من الفيزا وهي فيزا دراسة اي فيزا طالب او فيزا بروفيشنال وميزتها انها لا تحدد سبب سفره للهند من الممكن ان يكون علاج او دراسه او سياحه وتذهب وترى الوضع طبيعته ثم تحدد وجهتك والمعهد او الجامعة ثم يتم تحويل الفيزا كفيزا دراسة وهي ميزة قوية لهذه الفيزا ويوجد نوع ثالث وهي فيزا سياحية وتاتي لمدة اقصاها ثلاثة شهور ولكنها غير قابلة للتجديد لذلك جرة التنبيه لان اغلب يقع بهذه المشكلة ويتوقع انها سوف تجد ولللمعلومية كانت تجد ولكن بعد احداث مومبي اصبحت مستحيلة بالنسبة للطلاب القادمين من السعودية فعندهم مدينة جدة والرياض بالنسبة لرياض فهم متشددين اكثر بالنسبة لفيزا الدراسة ولا يعطون اكثر من ستة اشهر لطلاب اللغة لذلك يفضل الذهاب الى القنصلية في جدة

وكذلك الحصول على الفيزا من جدة لاتأخذ اكثر من يومين اما فالرياض عشرة ايام تقريبا

بالنسبة لدولة اليمن نفس الطلبات ولكن الاختاف فالضمانه البنكية كما هو اتى فالجزء التالي ولكن القبول لمعاهد اللغة يتم عن طريق معاهد معينة فلذا يجب السؤال وكذلك احب انبه على نقطة مهمة جدا ان السفارات يقبلون بالورقة الاصليه فقط لاغير حيث ان طبع الورقة وارسالها عن طريق الانترنت لايجدي نفعا في اغلب الاحيان

الضمانة البنكية

تختلف من دولة لاخرى حيث فالسعودية تعمل الضمانه البنكية من بنك ويفضل ان يكون من بنك الراجحي ولذلك بحكم قلة العمولة وتكون قيمتها سبعة الف سعودي بخطاب ضمانه موجه للسفارة الهندية

اما عن طريق اليمن فتكلفته خمسة وسبعين الف ريال يماني بما يعادل الف وخمس مئة ريال سعودي

رسوم الفيزا

رسوم الفيزا تقريبا نفسها في جميع الدول وهو مبلغ خمسة وسبعين دولار

صور شخصية

تقريبا اربعة صور شخصيه بمقاس صورة الجواز

تعبئة استمارات الطلب

يتم تعبئة استمارتين طلب يتم اعطائها للمتقدم وتكون باللغة الانجليزية وطبعاً يتم جلب الجواز الاصلي بالتاكيد

ويزيد لطلاب اللغة المقيمين بالسعودية ورقة من الكفيل موجه للسفارة لتسهيل الاجراءات وهو في هذه الحالة تكون من الوالد طبعاً لانه كفيل ابنه ويتم تخميمها من قبل الكفيل

بعدها يتم اعطائك وصل واعطائك موعد للقدوم واستلامها اما في بعض المدن كالرياض او جدة مثلاً لابد من مقابلة القنصل ليسالك بعض الاسئلة ويرى مدى جديتك في الدراسة

خطوات السفر

بعد استلام الفيزا يتم التأكد من تاريخ الانتهاء لانه يتم تغيير بعض التواريخ ولذلك جرى التنبيه

يتم التجهيز للسفر من خلال شراء بعض الحاجيات واهيب بالجميع بشراء قاموسين وهي قاموس اكفسورد الحديث للمفردات وكذلك القاموس المصور حيث انها مفيدة جدا

طبعاً البعض يفضل اخذ بعض الوجبات وهي مفيدة بصراحه كالأجبان لانها غالية بعض الشيء فالهند وان وجدت ليست بجودة اجبان الخليج اما الباقي فهو متوفر تقريبا ويتم الحجز عن طريق بعض الخطوط لوجود بعض العروض وارخص العروض على حسب المدينة المتوجه اليها كمدينة بنقلور تم فتح خط مباشر عن طريق الخطوط السعودية والسعر يعتبر مرضي بعض الشيء مقارنة ببعض الخطوط الاخرى للدول الاخرى ولللمعلومية ان تكلفة شراء تذكرة ذهاب وعودة من السعودية تعادل تذكرة ذهاب فقط من اليمن

الوصول للهند

يتم اعلام الشخص المستقبل بوقت الوصول لعمل الترتيبات اللازمة وعند حصول اي تاخير يتم اعلام الشخص المستقبل لحدوث بعض المشاكل بهذا الخصوص

فالطار لاتشعر بالخوف فهناك نقطتي وصول محتملة للهند اما بنقلور او حيدر اباد ولكن الاغلبية لينقلور بحكم تعلم اللغة سوف يجد المساعدة المطلوبة وسيتم اعطائه استارة خلال الرحلة يتم تعبئتها باللغة الانجليزية ومن هنا انبه ان تحمل معك قلم دائماً سوف تحتاجه فالهند والا سوف تجد التهزيء والاهانة تتم تعبئة الاستارة بكل سهولة ولايجال للخوف لانني اجد اغلب الطلاب يخافون منها فهي تطلب اشياء اساسية كمعلومات الجواز وهكذا ويطلب ايضا عنوان الإقامة فيتم سؤال زميلك عن عنوانه قبل المجيء لتعبئته والرجاء وضع العنوان والرقم الصحيح لانهم يتأكدون بعض الاحيان عن مدة صحة المعلومات

وعند استلام العفش ابحت في العفش عن اي علامة اكس بالابيض سيتم وضعها على الشنطة ومعناها انها سوف تفتح قبل الخروج من المطار وتفتش فعند وجودها حاول ان تبحث عن زاوية لايرك احد وامسحها بيدك او سوف يكون مابداخل الشنطة صيد ثمين لعمال الجمارك هذا مما رايته في مطار بنقلور

بعد الوصول واخذ قسط من الراحة يبدأ بعدها عناء البحث عن عائلة تتوفر لدى الطالب بعض الخيارات فيما يخص السكن، وتتلخص هذه الخيارات في الآتي:-

* **السكن الطلابي Students Hostels** يتوفر لدى معظم الجامعات والكليات سكن خاص للطلبة وآخر للطلاب. ولكن غالباً ما يكون الإقبال شديداً على هذا النوع وذلك نظراً لأن الرسوم التي تأخذ على الطلبة تكون منخفضة. ولذا فإن الطالب الراغب في الحصول على مكان في السكن الطلابي التقدم بطلب ذلك لجميع مسؤولي مباني السكن الطلابي حتى يضمن الحصول في أحدهم. وفي السكن الطلابي يجد الطالب نفسه بين بقية الطلبة القادمين من دول مختلفة

* **الإقامة مع عائلة Family Accommodation** أن بعض من الطلبة والطالبات يفضل السكن مع إحدى العائلات وذلك من أجل اكتساب اللغة الإنجليزية خاصة مع الأسر التي تستخدم اللغة الإنجليزية كلغة الحوار بين أفرادها، وكذلك من أجل ان تكفل هذه الأسر بالاحتياجات الأخرى مثل الأكل وغسل الملابس .. الخ

* **استئجار شقة Renting a Flat** يقوم معظم الطلبة باستئجار شقق قريبة من الكليات التي يدرسون فيها، وعادة ما يشترك مجموعة من الطلبة أو الطالبات باستئجار الشقة. وذلك من أجل العيش معاً وكذلك من أجل توزيع قيمة الإيجار عليهم جميعاً، والذي من شأنه تخفيف الأعباء المالية عليهم. وتختلف الإيجارات من منطقة إلى أخرى ومن بناءة إلى أخرى في نفس المنطقة الواحدة كما أن مساحة الشقة وعدد غرفها، وإذا كانت مؤثثة ام لا، كل هذه العوامل تؤثر على قيمة الأيجار. وتجدر الإشارة بأن أصحاب الشقق عادة يأخذون قيمة أجار 3 شهور مقدماً وذلك كنوع من الضمان **Deposit**، يعطى هذا المبلغ للطلبة بعد انتهاء مدة العقد الرسمي الذي يبرم بين الطرفين (صاحب الشقة والطلبة المستأجرين).

الإيجابيات وسلبيات الدراسة فاهند

من المؤكد ان الإيجابيات الدراسة فاهند اكبر من السلبيات وسوف نتحدث عن جانب اللغة مثلا لو ان طالب اراد دراسة اللغة وعنده وقت معين ومحدد بثلاثة اشهر للمثال فقط فالبعض يقول سوف اذهب الى منشأ اللغة كبريطانيا مثلا ولكن احسب التكلفة لثلاثة اشهر فقط مكلفة جدا وفالاساس ماهي هذه اللغة التي سوف نتجزها في ثلاثة اشهر المقصود من كلامي انه خلال ثلاثة اشهر بإمكانك انجاز مايمكن ان نتجزه في دولة بريطانيا ومن المستحيل اصلا ان تقول انه يمكنك ان تاخذ اللغة في ثلاثة اشهر وكذلك احسب التكلفة السعريه التي سوف يتم ادراجها في جزء كيفية التجهيز للسفر وكذلك ان درست في اي مكان فالمحرك والدافع الاساسي للتعلم لا بد ان يكون نابع من نفس الطالب لانه اذا وجدت الهمة والنشاط سوف ينجز الشئ الكثير والغير متوقع بمعنى ان اللغة تعتمد بشكل كبير على مجهودات الطالب بنسبة ستين الى سبعين بالمئة فتخيل معي ان الطالب كل يوم ياخذ درس يشمل قواعد ومفردات واشياء اخرى ولكن الطالب لا يحرك ساكنا من حيث مراجعته والقراءة والاطلاع واني اعرف بعض الطلاب يدرس لغة لثلاث سنوات فالكاتب من عنوانه ان كانت همتك دراسة سوف تنجز من الإيجابيات ايضا هو توفر الدورات في جميع التخصصات بأسعار خياليه بعض الاحيان وتختلف الاسعار على حسب المنطقة

وكذلك لانسى التكلفة ومدى رخصتها في بلد كاهند وهو عامل اساسي لمجيء الطلاب الجودة فالتعليم كذلك من اساسيات نجاح الهند في جلب الطلاب الاجانب وتسهيل العقبات لهم اغلب الاحيان ولكن يقابل ذلك بالبحر والاستهتار من بعض الطلاب العرب وتشويه السمعة اينما حل الطالب العربي ناقي للسلبيات والمشكلة ان الشر يعم والخير يخص بحيث انهم ينظرون لتصرفات طائفة لبعض الطلاب العرب وينسبونها للدين الاسامي وتحصل مشادات كثيرة بخصوص هذا الشئ

من السلبيات ايضا اقبال فكرة عن الهند انها فوق ماتتخيل القصد من حيث المعيشه والدراسة فالقصد ان اراد احد اخبار شخص عن الهند دعه يكتشف بنفسه واقصد انك لاتدعها بالحد الغير المعقول ثم ياتي الطالب وينصدم بالواقع وهذه تؤثر كثير فالطلاب ولمعرفتي لاشخاص كثر فبعضهم لم يطيل مدة تواجده في الهند ليومين او ثلاثة بالكثير وذلك لانه وصلته فكرة عن الهند غير التي شاهدها وطبعا لاتسال هندي عن الهند لانه سوف يشبهها بدي او جده

تجارب عملية لأشخاص سافروا إلى هناك (تجربة الأخ سعيد)

انا سأختصر تجربتي لمدة سنة في حيدر أباد لمدة سنة تتفوق حيدر أباد على بنقلور في ناحيتين رخص الدورات وزيادة نسبة المسلمين أفضل المعاهد في مجال الشبكات في حيدر أباد هم : زووم + نت ماتركس + أ. ظفر

ZOOM

الدورات التي ينصح بها : ccna - ccnp - mcitp

الإيجابيات:

- منظم ومرتب وكأنك في شركة راقية.
- دقه في المواعيد حيث ان كل كورس محدد تاريخ بدايته ونهايته بالتمام
- لابات ممتازة 100%
- سعر مناسب

السلبيات:

- سرعه التدريس
- مدة الدورة لا تكفي لتغطية المنهج بالكامل
- عدد الطلاب كثير نسبيا
- لا يقدم دورات متقدمه كالفويس والسيكيورتي وفي تقييمي هو افضل معه في حيدر أباد

في الصورة الموضحة الباكج الخاص

بزووم وهناك باجك آخر

لـ CCIE + CCNA + CCNP = 13000 روبية

الدورات التي ينصح بها :

ccna - ccnp - ccie

-ccsp -ccvp -ccip

الإيجابيات

- أ. صديق صاحب المعهد لديه

خبرة ممتازة وهو الافضل في حيدر

أباد

- يقدم دورات متقدمه في الفويس والسيكيورتي وغيرها

السلبيات :

- عدم الالتزام بالمواعيد

- عدد الطلاب اكثر من زووم

- عدم وجود لابات مناسبة

www.netmetric-solutions.com

في وجهه نظري هو ثاني معهد في حيدر اباد بعد زووم

بالنسبه لـ أ. ظفر فهو يدرس N+Wi-Fi, Advance Lan

يدرس في بيته وانصح أي شخص يدخل عنده مخلص في تدريسه يهتم بالجانب العملي أعدد الطلاب قليل ويأسس بشكل ممتاز

خبره تزيد عن 15 سنة في الشبكات ويعمل في شركة امريكية في الهايتك سيتي (مدينة الكمبيوتر في حيدرأباد)

اشارات

بإمكانك تأخذ الدورة أكثر من مرة في نفس المعهد او في معهد آخر مثل ما ذكر بعض الاخوة . المعاهد لاتغني ابداء عن المذاكرة الذاتية فهي الأساس الدورة تعطيك النقاط الاساسية وتسهل عليك فهم الكتب والفيديوهات وأخصه في الغربه غالبا اليوم بالكامل ملك لك

المعاهد تحاول تبرز الجانب الحسن فقط وتخفي النقاط السلبية .. بل أحيانا تقلب النقاط السلبيه الى إيجابيات .. مثلا يقولون لك شعارنا الدقه في المواعيد و التطبيق العملي .. فمجرد ان تدخل وتدف تجد العكس

هناك ما يسمه بالـ ديمو كلاس .. تحضر أول يوم ثم تقرر .. قد يكون حل نسبي للمشكلة

كذلك ليش شرط دفع كامل المبلغ .. بإمكانك تقسيطه على دفعات .. وهذا حل آخر

تجربة أخرى من الأخ خالد (تجربة مهمة)

أولا : المدينة الي انا كنت فيها وهي بنقلور ... (Bangalore) مدينة المعروفة في الجنوب في مقاطعة كارناتاكا (Karnataka) وطبعا كلامي رح يكون منحصر بواقع الدراسة في هذه المدينة والى عشته خلال فترة دراستي هناك

ومن المعروف عن هذه المدينة كثرة فروع الشركات العاليية وخاصة في مجال تكنولوجيا المعلومات .. وهي تعتبر عاصمة التكنولوجيا في الهند .. من بعدها تأتي مدينة حيدر أباد

يغلب على هذه المدينة طابع العمل وكثرة الوافدين سواء من الهند أو من خارجها والسبب يعود لتوفر فرص عمل كثيرة في هذه المدينة.

وبالنسبة لتكاليف المعيشة تتسم هذه المدينة عن غيرها من المدن الهندية الجنوبية بغلاء الاسعار نوعا ما ... (نسبيا)

أما بالنسبة للناحية العلمية ودراسة الشبكات فمن خلال دراستي في الهند التي كانت على اساس تجربة أحد الأصدقاء قبلي ... كان قد قدم إلى هذه المدينة ودرس في نفس المعهد ونصحني بالذهاب إلى الهند لدراسة الشبكات ... وجدت أنه من الصعب الحكم على الدراسة بالهند من خلال معهد أو اثنين أو ثلاثة .. فتوجد في هذه المدينة عدد كبير من المعاهد المتخصصة بمجال التكنولوجيا .. وعدد كبير منها في مجال الشبكات .. والأهم من ذلك أنه يوجد منها ما هو سيء ..

فمعظم المعاهد هناك تعتمد على اساس إعطاء الدورات بأسعار رخيصة جدا .. ولكننا من ناحية أخرى لا توفر مدرس متمرس لتدريس هذه الكورسات .. وإني تكتفي بأحضر شاب قد أتم هذه الشهادة و تعتبره مؤهلا لإعطاء هذه الدورات

والناحية الأخرى السلبية في بعض المعاهد هي اعتدائها على السرعة .. وهذا موجود أيضا في وطننا العربي .. حيث ان دورة CCNA مثلا يمكن إنهاؤها في اسبوع واحد فقط (Boot Camp) اربع أو خمس ساعات يوميا ... مع العلم ان هذه الشهادة يجب أن تعطى أكثر من ذلك بكثير من ناحية الوقت .. ولا يمكن أنجازها بهذه المدة البسيطة إلا على حساب المادة العلمية وتجاوز بعض النقاط ..

الناحية الأخرى : هي المال (Money)

معظم المعاهد الهندية تحاول اقناع الدارس انه يجب دفع كامل المبلغ قبل بدء الدورة ... وهذا ما أحذر منه بشكل شديد لانني لم افعله والحمدلله والفضل يعود لصديقي الذي لفت نظري بعدم دفع اي مبالغ مقدما .. وأنا دفع المبالغ على دفعات .. حتى انهاء الكورس

وذلك لانهم بمجرد حصولهم على المال .. لا يباليون بأي طلبات قد تطلبها أثناء أخذ الكورس .. بالإضافة الى عملية تغيير مواعيد الكورسات الاخرى على حساب موعده .. اذا قمت بالدفع سلفا .. وغيرها الكثير

هناك ناحية سلبية أخرى وهي عدم تقيد المديرين بالمواعيد .. وذلك يعود الى طبيعة بشرية متأصلة في بعضهم وليس كلهم ... (هذا ما لاحظته)

هناك نواحي إيجابية عديدة ؟... ولكني لا أرى أنها إيجابية بحتة ؟... وذلك لان النواحي السلبية قد تغلب على النواحي الايجابية مما يجعلها تفقد الكثير .. ولأن الحياة الصعبة التي قد تواجهها (صعوبة العيش .. من صعوبة الطعام ... كثرة القذارة .. بيئة المدينة الملوثة .. وغيرها) تجعل من الدراسة الذاتية الحل الأمثل والأرخص لكثير من الشباب الجاد في الحصول على المعرفة ... هذا ما توصلت اليه متأخرا ... مع الاسف

انا لا اقول انني لم استفد من شئ .. بالعكس فقد تعلمت الكثير .. وتعرفت على مدرسين ممتازين ولكن الاهم من ذلك ... هو انه لايمكن انا اعطيك المدرب (مهما كان متمرسا) أكثر من الذي تستطيع الوصول اليه بقليل من التعب ... وأرى ان هذا التعب .. مهما كان كبيرا .. ولكنه نافع .. أما من ناحية توافر المخابر (LABS) فالمعهد الذي كنت ادرس فيه يحتوي على لاب ممتاز نوعا ما .. واستطيع التدريب عليه في اي وقت شئت بذلك .. ولكن لا ارى أن هذا اللاب أكثر مما يستطيع تقديمه الـ GNS .. في معظم الأحيان

أما من حيث نصيحتي للراغبين بالدراسة بالهند فهي ...

لن تعطيك الهند اكثر من الذي تستطيع انت الحصول عليه ...

MCITP - 2008

PROFESSIONAL IT PROFESSIONAL

Duration: 1 Month (10 days on 10th of every month)

CCNA

COMPUTER NETWORKING

Duration: 15 Days (10 days on 10th & 10th of every month)

RHCE LINUX / UNIX

COMPUTER NETWORKING

Duration: 1 Month (10 days on 10th & 10th of every month)

EXCHANGE SERVER

COMPUTER NETWORKING

Duration: 15 Days (10 days on 10th & 10th of every month)

PC HARDWARE & NETWORKING

COMPUTER NETWORKING

Duration: 15 Days (10 days on 10th & 10th of every month)

ETHICAL HACKING + NETWORK SECURITY

COMPUTER NETWORKING

Duration: 15 Days (10 days on 10th & 10th of every month)

CCNP

COMPUTER NETWORKING

Duration: 1 Month (10 days on 10th & 10th of every month)

CCIE

COMPUTER NETWORKING

Duration: 1 Month (10 days on 10th & 10th of every month)

Advanced FIREWALL

COMPUTER NETWORKING

Duration: 15 Days (10 days on 10th & 10th of every month)

Special Offer

All 5 Courses just for Rs5,500/- Only

10.3 % TAX Extra

PROMETRIC

Microsoft Certified Partner

ZOOM TECHNOLOGIES

أصدار جديد من برنامج GNS3



أصدار جديد من برنامج Packet Tracer

Cisco Packet Tracer
5.3



أصدرت سيسكو مؤخرًا الأصدار الكامل لبرنامج الباكيت ترايسير في إصداره 5.3 والجدير ذكره أن هذا النسخة قد صدرت أكثر من مرة لكن في نسخة بيتا وكان يعمل لفترة محدودة تصل شهر واحد وأفضل خبر في هذا الأصدار هو دعمه لبعض الأمور الخاصة بشهادة **CCNP** مثل دعمه لبروتوكول الـ **BGP** والكثير من الإضافات المتنوعة وهذه لائحة بقائمة الإضافات الجديدة

Improved Linksys models, added WEP wireless security algorithm, Cable and DSL enhancements
Call Manager Express (VOIP support)
FTP server and routers/switches – server and client
Email system (SMTP and POP3) – server and client
Border Gateway Protocol (BGP) – limited implementation that allows for a more realistic representation of the Internet for scenarios
Generic IP end devices – to create more versatility in device creation
Activity Wizard Initial Tree enhancements – more scenario variations
The new protocol support and activity wizard enhancements in version 5.3 will enable instructors to teach concepts in CCNA Discovery, CCNA Exploration, and CCNP courses more effectively, including the following:

CCNA Discovery

Networking for Home and Small Businesses:
Improved Linksys models and wireless security protocols and algorithms, generic IP end devices
Working at a Small-to-Medium Business or ISP:
Better DNS, improved DHCP, wireless security, new FTP, SMTP, POP3

Introducing Routing and Switching in the Enterprise: Improved multi-area OSPF, EIGRP, BGP
Designing and Supporting Computer Networks:
New VOIP, Call Manager Express

CCNA Exploration

Network Fundamentals: Improved HTTP, DNS, DHCP; new FTP, SMTP, POP3
Routing Protocols and Concepts: Improved multi-area OSPF, EIGRP, new BGP
LAN Switching and Wireless: Improved Linksys models, wireless security algorithms, 802.11
Accessing the WAN: New PPPoE, enhanced IPSec, Cable and DSL enhancements

CCNP

Improved multiarea OSPF, EIGRP, new BGP

أعلن موقع الـ **GNS3** عن إصدار جديد للبرنامج تحت رقم **0.7** ونجد فيها الكثير من الإضافات الجديدة مثل أداة **Qemu** و **putty** بالإضافة إلى إصدار جديد من برنامج الدايناميس كما تم إصلاح الكثير من الثغرات فيه وهذه قائمة بجميع التحديثات والإضافات الجديدة

- * Support & debugging on Windows 7.
- * Qemuwrapper improvements & Windows compatibility.
- * Integration of Cisco IDS/IPS, including a new symbol.
- * Qemu 0.11.0 patched and Putty have been added in the Windows all-in-one package.
- * An option to show the z coordinate of any object on the scene (View -> Show layers).
- * Interface labels follow their moving parent nodes.
- * Modified interface labels are saved in .net files.
- * Option to slow start nodes (wait x seconds between each start).
- * Links connected to Qemu based nodes are now removable (nodes have to be shutdown to do so).
- * Possibility to set an hypervisor for Ethernet switches, ATM switches, ATM bridges and Frame Relay switches.
- * New symbols for voice labs (Call manager, SIP server, IP phone, voice router, voice access server and PBX).
- * New dialog window to browse and change a router startup-config.
- * Undo/redo of actions is now supported.
- * Qemu & qemu-img paths are saved in .net files if needed.
- * Slight improvements for the snapshot system, including a new dialog window to manage it.
- * Wics description in tootips.
- * Wics restoration from .net files.
- * Support of relative paths in .net files (if the base path is the same as the .net file).
- * Test button to validate you can launch Qemuwrapper, Qemu and qemu-img.
- * New translation in Czech (thanks to Ondrej Filip).
- * Lot of various small bug fixes and improvements.

كيفية إستعادة كلمة السر لأجهزة جونيير؟

أعداد: أيمن النعيمي



أحد السياسات التي تتبعها الشركات المصنعة للأجهزة المنظمة لعمل الشبكات هو تأمين طريقة تسمح للمستخدم بأسترجاع كلمة السر في حال فقدانها أو قرصنتها لذا اليوم سوف نطرح في هذا المقال الطرق التي وضعتها جونيير لأستعادة كلمة السر في حال فقدانها ويجب أن نعلم أن جونيير تعتمد طريقة لكل نوع من أجهزتها وأقصد بكلمة نوع هو نوعية الجهاز نفسه وهذا يشمل طريقة للروتر وطريقة للسويتش وطريقة للفايروول وقبل أن نبدأ يجب أن نتفق على أن أستعادة كلمة السر تتم دائما عن طريق Console Port مثلها مثل اجهزة سيسكو وهذه الصورة توضح طريقة الاتصال بين الكمبيوتر والجهاز بشكل عام

ننتظر قليلا وبعدها نكتب كلمة Recovery

```
sio0: type 16550A, console
sio1: configured irq 5 not in bitmap of probed irqs 0
sio2 at port 0x2f8-0x2ff irq 3 on isa0
sio2: type 16550A
sio3: configured irq 7 not in bitmap of probed irqs 0
DEVFS: ready to run
ad0: 8192MB <VMware Virtual IDE Hard Drive> [17753/15/63] at ata0
ata2-master: <VMware Virtual IDE CDROM Drive/00000001> CDROM device

Mounting root from ufs:/dev/ad0s1a
if_pfe_open: listener socket opened, listening...
Mounted jbase package on /dev/vn0...
/packages/mnt/jbase/etc/rc.single: Can't open /packages/mnt/jbase.
No such file or directory
System watchdog timer disabled
Enter full pathname of shell or 'recovery' for root password recovery
for /bin/sh: recovery
```

وبعدها ندخل على CLI وندخل على configuration mode بواسطة الأمر `config-re` ونقوم بوضع كلمة سر جديدة للـ `Root` بواسطة الأمر التالي `set system root authentication plain-text password` والصورة توضح جميع الاوامر ولاننسى آخر امر لحفظ العمل وهو `commit and quit`

```
NOTE: exit
NOTE: When you exit the CLI, you will be asked if you want to reboot the system
Starting CLI ...
root>

root> configure
Entering configuration mode

[edit]
root# set system root-authentication plain-text-password
New password: NewPassword
Retype new password: NewPassword

[edit]
root# commit and-quit
```

وأخر شيء نخرج من الـ `Recovery mode` بواسطة الأمر

إستعادة كلمة السر للسويتشات من نوع EX Series

استعادة كلمة السر في السويتش تختلف قليلا عن الروتر وسوف نعلم على اولا الخطوات التي قمنا بها في الروتر بعد كتابة الأمر `Boot-S` سوف نحصل على هذه الرسالة :

Enter full pathname of shell or 'recovery' for root password recovery or RETURN for /bin/sh:

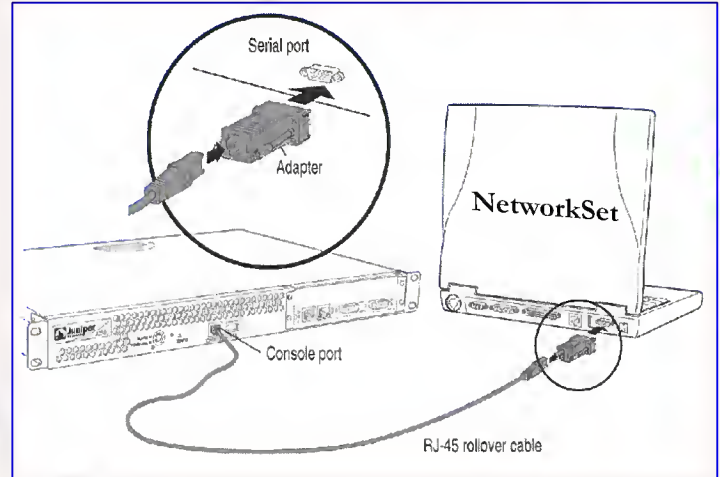
لا نقم بكتابة اي شيء فقط أضغط `Enter` وبعدها ننفذ الاوامر التالية لكي نقوم بحذف كلمة السر نهائيا

```
mount -a
# rm /config/juniper*
# exit
```

وبعدها سوف ندخل على السويتش بواسطة الـ `root` وبدون كلمة سر والسبب لاننا قمنا بحذف الملف الذي يتم تخزين فيه كلمة السر

وأخيرا بالنسبة لاستعادة كلمة السر في الفايروول

لايوجد أي طريقة لاستعادته كم هو موضح من جونيير والحل الوحيد هو إعادة الفايروول الى حالته الاولى اي `factory default settings` وطبعاً هذا سوف يؤدي الى ازالة كل الإعدادات الخاصة بك في الفايروول



إستعادة كلمة السر للروتات من نوع J Series

نقوم أولاً بإغلاق الروتر ونقوم بنوصيله كما هو موضح بالصورة ونستخدم `Adapter` خاص للتحويل من `RJ-45` الى `DB-9` ونستخدم أحد البرامج للاتصال كالـ `Hyper Terminal` ونحدد سرعة الكونسول بي و9600 نقوم بتشغيل الروتر بعدها وننتظر حتى تظهر لنا هذه الرسالة

Hit [Enter] to boot immediately, or space bar for command prompt.

Booting [kernel] in 9 seconds

وعندها نقوم بالضغط على `Space` كما هو موضح في الرسالة للدخول على `command prompt`

```
Uptime: 2m42s
ata0: Spinning down devices. Please wait...
ata2: Spinning down devices. Please wait...
Rebooting...
Console: serial port
BIOS drive A: is disk0
BIOS drive C: is disk1
BIOS 638kB/260032kB available memory

FreeBSD/i386 bootstrap loader, Revision 0.8
(builder@ryowo.juniper.net, Fri Oct 21 00:52:35 GMT 2005)
Loading /boot/defaults/loader.conf
/kernel text=0x4084a1 data=0x3530c+0x5608c syms=[0x4+0x4a670+0x4+0
Hit [Enter] to boot immediately, or space bar for command prompt.
Booting [kernel]...
```

نقوم بكتابة الأمر التالي `Boot-S`

```
sio0: type 16550A, console
sio1: configured irq 5 not in bitmap of probed irqs 0
sio2 at port 0x2f8-0x2ff irq 3 on isa0
sio2: type 16550A
sio3: configured irq 7 not in bitmap of probed irqs 0
DEVFS: ready to run
ad0: 8192MB <VMware Virtual IDE Hard Drive> [17753/15/63] at ata0
ata2-master: <VMware Virtual IDE CDROM Drive/00000001> CDROM device

Mounting root from ufs:/dev/ad0s1a
if_pfe_open: listener socket opened, listening...
Mounted jbase package on /dev/vn0...
/packages/mnt/jbase/etc/rc.single: Can't open /packages/mnt/jbase.
No such file or directory
System watchdog timer disabled
Enter full pathname of shell or 'recovery' for root password recovery
for /bin/sh: recovery
```


أربعون سنة تمر اليوم على الانترنت

وضعت شبكة الانترنت عام 1969 الأساس لما هو معروف الآن بأنه أحد أهم أدوات التاريخ الإنساني.



التاسع والعشرون من شهر أكتوبر عام 1969 في تمام العاشرة والنصف مساءً، كانت ولادة الانترنت. كان الباحثون في وكالة مشاريع البحث المتقدم التابعة لوزارة الدفاع يحاولون التوصل إلى طريقة لربط مجموعة من أجهزة الكمبيوتر البعيد بعضها عن بعض داخل شبكة واحدة. وتحديدًا منذ أربعين عامًا تم إنشاء أول شبكة من هذا النوع عرفت باسم "أربانت" حيث تم ربط مجموعة من أجهزة الكمبيوتر داخل جامعة كاليفورنيا بولوس أنجلوس، مع مجموعة أخرى بمعهد ستانفورد للبحوث. إنه من المفترض أن تكون أول رسالة تبيت على الشبكة هي كلمة "دخول". عملت الشبكة جيدًا، ونقلت الرسالة خلا حرف "د" و حرف "خ" بدون مشاكل، إلا أنها تحطمت عند حرف "و". ومع نهاية عام 1969 كانت الشبكة تربط أربعة أجهزة كمبيوتر معا. هذا الاتصال كان الأساس لما أصبح - بعد أربعة حقب من الزمان - أحد أهم أدوات التاريخ الإنساني.

التسعينيات

خرجت شبكة الإنترنت بشكلها الحالي إلى النور في التسعينيات. ظهرت أول صفحة على الشبكة العنكبوتية في عام 1991 وكان الهدف منها وقتها هو شرح لعنى صفحة (ويب بيج) ثم بدأت الصفحات تأخذ المستخدم من رابط إلى آخر عن طريق ضغطه على عنوان الرابط، وبعدها بدأ المستخدمون في تحميل محرركات بحث مثل "نتسكيب نافيجيتور"، وبدأت الطفرة الهائلة في الشبكة العنكبوتية. فمن بداية الحقبة كان هناك حوالي 300000 جهاز كمبيوتر متصل بالشبكة ليصل هذا الرقم إلى 52 مليون جهاز مع نهاية الحقبة. وهذا النمو السريع خلق واحدة من أكبر الفقاعات الاقتصادية في التاريخ الحديث، وبدأت المشاريع الخاصة بالشبكة العنكبوتية تنشئ سوقًا رأسماليا هائلًا على أنقاض البورصات المنهارة.

عام 2000 وما بعده

مع بداية الألفية الجديدة انفجرت فقاعة التكنولوجيا واختفت مليارات الدولارات من السوق، وأصبحت الانترنت الأداة الأساسية للبحث والعمل. وكانت كل الاختراعات الخاصة بالانترنت منذ عام 2000 تستهدف المستخدم أولاً - من الويكيبيديا إلى الفيسبوك وصولاً إلى سكايب. وظهرت غوغل كواحدة من أهم محرركات البحث على شبكة الانترنت، وظهرت شبكات كثيرة على الانترنت تتاجر في كل السلع بدءاً من التيشيرت وصولاً إلى العقارات، وذلك بفضل التكاليف الضئيلة جداً لإنشاء أي شركة تجارية عن طريق الانترنت. كما تطورت الانترنت لتصبح من أهم وأقوى الأدوات التي يستخدمها السياسيون أيضاً؛ فالكل أصبح يستخدم الانترنت.

الاتصال

في بداية ظهورها كانت الانترنت تتكون فقط من "مضيفين" - وهو المعنى التقني لتوصيل الأجهزة بالشبكة. وعلى مدار أربعين عامًا اتصل بالشبكة أكثر من 700 مليون جهاز، أي أن أكثر من جهاز كمبيوتر متصل بالشبكة كل ثانية على مدار أربعين عامًا. إلا أن الحقبة الأخيرة هي الأكبر من حيث انتشار الشبكة في العالم حيث زاد عدد الأجهزة المتصلة بالشبكة العنكبوتية من 93 مليوناً، إلى 700 مليون جهاز في العالم.

معدل استخدام الانترنت في 30 يونيو 2009

المكان	النسبة المئوية للسكان	العدد بالمليون
العالم	24.7%	1.6 مليار
شمال أمريكا	251.7%	73.9 مليون
أمريكا اللاتينية/الكاريبي	175.8%	30.0 مليون
الشرق الأوسط	26.7%	74.5 مليون
آسيا	704.2%	18.5 مليون
أستراليا	60.1%	20.8 مليون
أفريقيا	65.9%	6.7 مليون
أوروبا	51.7%	375.9 مليون

السبعينيات

شهدت السبعينيات انتشاراً كبيراً بالأربانت في مختلف الجامعات بالولايات المتحدة. أما في مختلف أنحاء العالم فقد كان الباحثون والوكالات الحكومية عاكفين على محاولة إنشاء شبكة مماثلة بمواصفات تقنية متعددة. فبدلاً من وجود شبكة واحدة، أصبح هناك عدة شبكات صغيرة. كما شهدت السبعينيات أيضاً ولادة البريد الإلكتروني. كما بدأ استخدام الرمز @ في العناوين البريدية بالإضافة إلى إنشاء بعض الخواص الأخرى للبريد الإلكتروني. وبنهاية السبعينيات بدأت الانترنت تخرج من نطاق الاستخدام البحثي إلى المستخدمين العاديين. ومع نهاية تلك الحقبة أصبح البريد الإلكتروني يستعمل عن طريق أعداد كبيرة من المستخدمين.

الثمانينيات

بالرغم من وجود تنافس كبير في مجال تكنولوجيا الشبكات في مختلف أنحاء العالم، إلا أن الباحثين كانوا يفضلون البروتوكول الخاص بالأربانت. وبالفعل أصبح هذا البروتوكول هو النظام الأساسي للانترنت في النهاية. كما بدأت الشبكات الاجتماعية في الظهور، وشهدت الثمانينيات ظهور (موديم) أسرع، حيث كان المستخدم يدخل ويتصل بالشبكة مباشرة. ومع نهاية الحقبة استطاع مطور فنلندي إنشاء أول "سيرفر" في العالم يدعم نظام الدردشة (الشات) الذي أصبح فيما بعد أساس برامج الدردشة (الشات) في العالم.

اللغات المستخدمة على الإنترنت

اللغة	ملايين المستخدمين	النمو 2000-2009
العربية	49.3	1.862%
الروسية	38	1.126%
الصينية	361.3	1.109%
البرتغالية	73	864%
الاسبانية	133	631%
الفرنسية	76.9	531%
الانجليزية	478.7	237%
الألمانية	65.2	136%

السنة	عدد الأجهزة على الشبكة
1969	4
1970	13
1975	62
1980	188
1985	1961
1990	313000
1995	6642000
2000	93047785
2005	394991609
2009 (الي يوليو)	681064561

*نقلًا عن "غلوب آند ميل" البريطانية

نتائج الأستفتاء الشهري

نتائج الأستفتاء

ماهو أنطباعك حول دراسة الشبكات في الهند؟

● حسب المكان والمعهد

59% ☐

● ممتازة

25% ☐

● سيئة جدا

6% ☐

● جيدة

5% ☐

● سيئة

5% ☐

الأستفتاء الأخير الذي قمت به على المدونة كان حول معرفة أنطباع العرب حول دراسة الشبكات في الهند وأنا كمصوت صوت على خيار سيئة مع أن أغلب المصوتون قد صوتوا أن الدراسة ممتازة وهي تختلف بحسب المكان واسم المعهد ولكن لوجهة نظري هناك أسباب وأحد أهم الأسباب هو عامل الوقت الذي يتم فيه تقديم وشرح الكورس فمثلا لو أخذنا شهادة مثل CCNA فهي تحتاج منك في الهند للحصول عليها أسبوعان فقط !!! وهذا برائي شيء من الخيال فشهادة مثل CCNA تحوي من المعلومات والمبادئ بحيث يصعب على أي شخص أن ينتهي منها في أسبوعان وخصوصا أن هذه الشهادة هي أول شهادة سوف تعرفك على سيسكو وعلى أجهزتها وطبعا الدارس لهذه الشهادة لا يملك أي خلفية في هذا الموضوع حتى تساعده على فهم هذه الكورس في أسبوعان فقط وأجد البعض يقول لي أن الدراسة في الهند تعتمد بنسبة كبير على الطالب وهنا عدنا لنقطة البداية وهي إذا كان الاعتماد الأكبر على جهد الطالب فالأفضل له أن يجلس في البيت ويدرس بنفسه Self Study من خلال الكتب والفيديوهات المتوفرة ولا يجبر نفسه على الاغتراب والتعب وقد طرحت في الموضوع الخاص بالهند تجربة مهمة مرت بأحد الأصدقاء وهو أخبرني بشيء مهم وهو **لن تعطيكم الهند أكثر من الذي تستطيع أن تحصل عليه بنفسك**

النقطة الثانية وهي لماذا نحن كدول عربية لانقوم بعمل هند عربية على أرضنا من خلال افتتاح مراكز مجهزة بكل المعدات والكوادر القادرة على إعطاء هذه الكورسات والدورات وبأسعار مناسبة وأخص مصر بهذه النقطة لان مصر هي التي تملك أفضل المعطيات على الساحة العربية وحتى لو قمنا بجلب أساتذة هنود لكي يدرسوا في معاهدنا فهي فترة زمنية وبعدها نبدأ بالاعتماد على كوادرنا العربية ولا ننسى اعتماد اللغة الانكليزية كلغة تدريس أساسية فهي أحد الأسباب التي تدفع الطلاب للسفر إلى الهند .

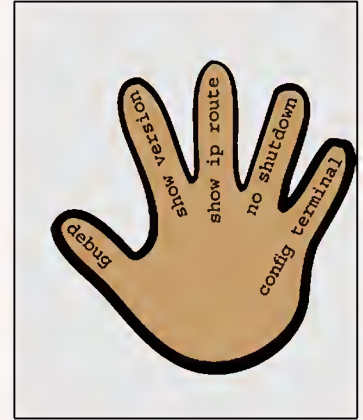
شجع هذا النوع من المجالات

بوضع أعلانك هنا

عشرة أوامر يجب أن يعرفها أي مهندس يعمل على أجهزة سيسكو



كما هو معروف عند أي شخص تعامل مع أجهزة سيسكو روتر كان أو سويتش أو جدار ناري أن نظام التشغيل المطور من قبل سيسكو IOS يحوي آلاف الأوامر التي من الصعب حفظها لذا سوف أطرح أهم عشرة أوامر والتي تعد الحجر الأساس والتي يجب على كل شخص محترف ومبتدأ في سيسكو أن يعلمها ويحفظها ويستفيد منها أثناء تعامله مع نظام IOS



الأمر السادس config terminal enable interface and router

في روترات سيسكو هناك عدت وضعيات أو Modes ونقطة الاختلاف الرئيسية هي الصلاحيات الموجودة بالإضافة إلى الاوامر المتاحة فعند تشغيل الروتر سوف نجد هذه الإشارة "<" وهي تدل على أنك في وضعية الـ User Mode لذا نقوم بكتابة الأمر enable لندخل على الـ Privileged Mode والذي يتيح لنا ان نشاهد كل مانريده على الروتر من دون القيام بعمل أي تغيير وهو يستخدم هذه الإشارة للدلالة على وضعية الـ "#" وللقيام بأي تغيير سوف نطرح ان ندخل على وضعية ذات صلاحية أكبر تسمح لنا بعمل التغييرات على الروتر وهي الـ Global Configuration Mode وهي تكون بهذا الشكل #config أما في حال أردنا أن نقوم بعمل تغييرات على أحد البورتات مثل إعطاء عنوان أيبى فيجب علينا أن نتوجه إلى الـ Interface Mode من خلال كتابة الأمر interface وبعددها نضيف رقم البورت وهو يكون بهذا الشكل #config-if وأخيرا للأعداد الـ Protocol Routing على الروتر سوف نستخدم الأمر router مسبوقا بنوع البروتوكول وهو يكون على الشكل التالي #config-router وذاتنا نستخدم الأمر exit للخروج من أي وضعية نحن فيها.

الأمر السابع no shutdown

هذا الأمر يقوم بتفعيل البورت أو يقوم بتشغيله ويتم من خلال الدخول على الـ interface mode وهو من الأمور الأولى التي يجب التأكد منها في حال عمل تشخيص لمشكلة على البورت ويمكن اختصار هذا الأمر إلى no sh.

الأمر الثامن show ip route

أيضا من الأوامر المشهورة وهو يقوم بعرض الـ Routing Table وهي عبارة عن قائمة تحوي كل الشبكات التي يمكن للروتر أن يصل إليها وكيف يستطيع الوصول إليها ويمكن اختصار هذا الأمر إلى sh ip ro لأزالة كل المعلومات الموجودة في هذا الأمر نستخدم الأمر التالي clear ip route

الأمر التاسع show version

هذا الأمر يقوم بأعطاءك تفصايل مهمة عن الروتر مثل الـ configuration registryIOS, version IOS name وحجم الـ ram والفلاش الموجود ويمكن اختصاره إلى sh ver

الأمر العاشر debug

لهذا الأمر أمكانات كبيرة وخيارات كثيرة وخصوصا في مسألة الـ Trouble-shooting فهو يقوم بعرض حالة أي خدمة أو بروتوكول يعمل على الروتر مثل eigrp, aaa, frame relay ومثال على الأمر debug ip route وهو يقوم بعرض كل الشبكات التي تضاف أو تزال من الـ Routing table.

الأمر الأول "?"

أحد أهم الأشياء التي يجب ان تعرفها هي إشارة الاستفهام "?" وهي عادة تستخدم لطلب المساعدة من سيسكو IOS وبشكل مختلف عن باقي أنظمة التشغيل التي تستخدم كلمة Help للمساعدة ولهذا الأمر عدة طرق للاستخدام الأولى: عندما لا تعلم ماهو الأمر الذي تريده أو أنك لاتذكره لذا قم بكتابة إشارة الاستفهام في موجه الأوامر ليقوم IOS بعرض كل الأوامر المتاحة في الوضع الذي أنت فيه Privilege Mode , Configuration Mode , Inter-face Mode الثانية: عندما لاتعلم ماذا يجب كتابته بعد الكلمة الأولى أو الثانية من الأمر مثل أن نكتب Show ip route ? و ليقوم بعدها IOS بعرض كل الخيارات المتاحة بعد هذه الأمر.

الأمر الثاني show running-configuration

يستخدم هذا الأمر تقريبا على كل أجهزة سيسكو روتر كان أو سويتش أو جدار ناري ويستخدم في معرفة الأعدادات الحالية للجهاز والتي يعمل الآن من خلالها وضم على ذلك أن هذه الأعدادات لاتخزن على الذاكرة وهي مؤقتة فقط حتى تقوم أنت بحفظها من خلال الأمر copy running-configuration startup-configuration ويمكن اختصار هذا الأمر إلى show run

الأمر الثالث copy running-configuration startup-configuration

وظيفة هذا الأمر هي حفظ الأعدادات الحالية التي تم التطرق لها في الأمر السابق والتي تكون محفوظة على الـ ram RAM إلى الذاكرة المسؤولة عن حفظ الأعدادات وهي الـ NVRAM وهذا الأمر مهم لان في حال قمنا بعمل إعادة أفلاخ للجهاز أو حدث انقطاع في الكهرباء فأن الجهاز سوف يقوم باستعادة كل الأعدادات التي قمنا بتجهيزها من الـ NVRAM ويمكن اختصار الأمر إلى copy run start كما يمكننا إرسال نسخة من الأعدادات إلى سيرفر TFTP

الأمر الرابع show interface

هذا الأمر يقوم بعرض حالة البورتات الموجودة على الروتر والتي تتضمن حالة البورت هل يعمل أم لا حالة البروتوكول على البورت بالإضافة إلى الأخطاء وكيف يستخدم البورت والـ MTU يعد هذا الأمر مهم جدا في تشخيص الأخطاء وحل المشاكل وهو مدعوم من خلال الروترات والسويتشات.

الأمر الخامس show ip interface

وهو من أشهر الأوامر وهو يكتب بهذا الشكل show ip interface أو بهذا الشكل show ip interface brief الأول يقوم بعرض الكثير من المعلومات حول حالة الأيبى بروتوكول على جميع البورتات وحالة المنفذ بشكل عام والأمر الثاني يقوم بعرض سريع لحالة البورت والأيبى المستخدم ويبين الأخطاء التي يمكن ان تحدث على الطبقة الأولى والثانية.

ماذا أفعل لو في حال نسيت كلمة السر الخاصة بالدومين؟

بقلم: أيمن العجمي

لنقم الآن بتشغيل موجه الأوامر ونقوم بكتابة الأمر التالي (سوف أشرح الخطوات الآن وفي الآخر سوف أشرح كيف تمت العملية بالتفصيل)

instsrv.exe FixPass "c:\recovery\srany.exe"

```
C:\recovery\cmd.exe
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

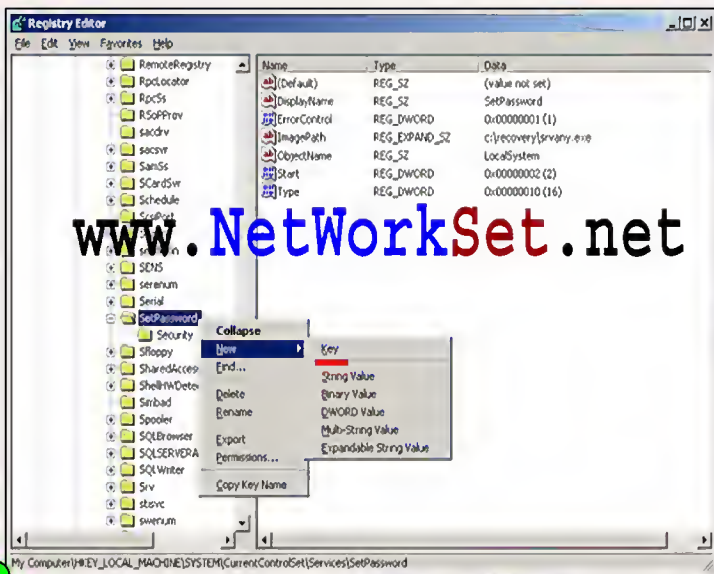
C:\recovery>instsrv.exe SetPassword "c:\recovery\srany.exe"

The service was successfully added!

Make sure that you go into the Control Panel and use
the Services applet to change the Account Name and
Password that this newly installed service will use
for its Security Context.

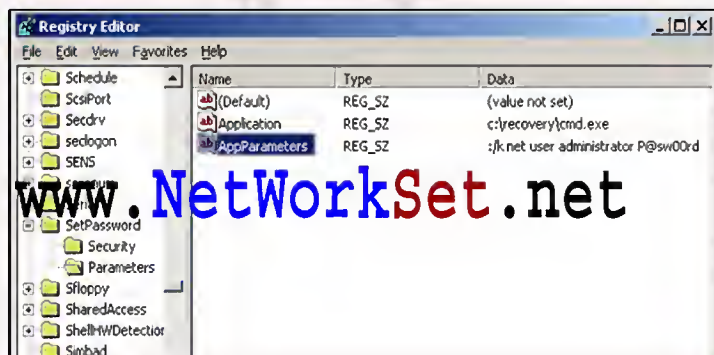
www.NetworkSet.net
C:\recovery>
```

الخطوة القادمة سوف نتوجه فيها إلى الريجستري وعلى الأمتداد التالي **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\SetPassword** ونقوم بإنشاء مفتاح فرعي بأسم **Parameters** ونبدأ بأضافة القيم التالية بداخله (أرجو مراعاة كل حرف وكل كلمة حتى نتجح الطريقة بشكل جيد)



القيمة الأولى **Application** وبداخلها نكتب السطر التالي **c:\recovery\cmd.exe**

القيمة الثانية **AppParameters** وبداخلها نكتب السطر التالي **/k net user administrator P@sw00rd** مكان كلمة **P@ssw00rd** ضع كلمة السر الجديدة للدومين وهذه صورة توضيحية لكل الإضافات



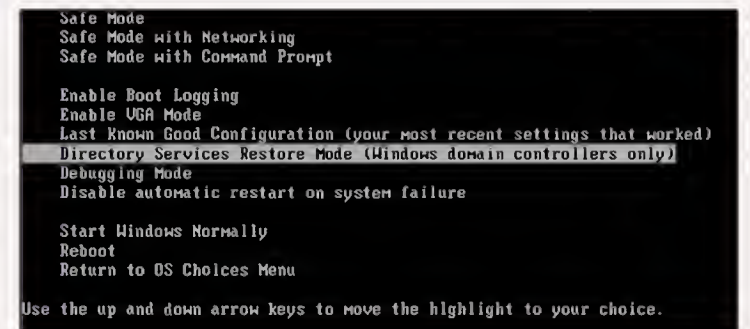
قد تكون مسألة نسيان كلمة السر للدومين شيء مستحيلا كون الموضوع قد يسبب مشاكل كثيرة للشركة ولكن القاعدة العامة تقول لا يوجد شيء مستحيل فقد ينسى مدير الشبكة كلمة السر أو قد يتعرض للاختراق من داخل أو خارج الشبكة ويتم تغيير كلمة السر للدومين وهذا ماحدث لأحد أصدقائي إذا ما الحل؟

القصة بدأت باتصال من أحد الأصدقاء وقال لي ان أحد الأشخاص الذين يعملون معه قد قام بتغيير كلمة السر الخاصة بالدومين أثناء عدم تواجده وانه الآن لا يستطيع الدخول إلى الدومين مما أدى إلى توقف العمل لديه وطلب مني المساعدة لحل المشكلة وأول خيار خطر على بالي هو استخدام سيدي **Hiern Boot** فهو يحوي باقة من الادوات تساعد في هذا الموضوع إلا ان السيدي لم ينفع بأي شيء إذا ما هو الحل ولماذا السيدي لم ينفع؟؟؟

لنتفق أولا على شيء مهم وهو أن كل أنظمة التشغيل الخاصة بي مايكروسوفت تقوم بحفظ أسماء المستخدمين وكلمات السر الخاصة بهم في ملف يدعى **SAM** وهو موجود على الرابط التالي **c:\windows\system32\config\By Default** وهو الملف التي تلجأ له كل البرامج الموجودة على السيدي لتغيير أو حذف كلمة السر لنظام التشغيل لكن لتتوقف قليلا **كلمة السر الخاصة بالدومين لا تحفظ في ملف السام بل تحفظ في الريجستري وبطريقة مشفرة ومعقدة** إذا ما الحل؟

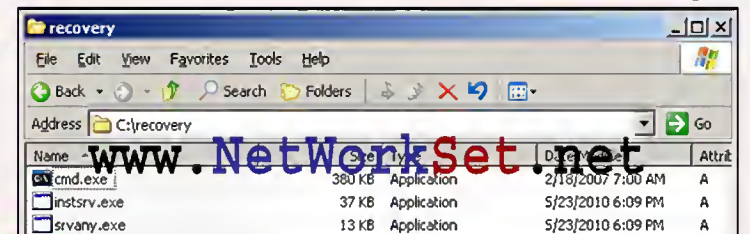
توجهت إلى محرك البحث غوغل والصرحة أنا أعد نفسي محترف بحث لكن تفاجئة أن نتائج البحث لاتعطي أي طرق وأغلب النتائج كانت عبارة عن برامج وأدوات غير نافعة وكان تصوري أنني سوف أشاهد الحل في أول نتيجة لكن لاشيء وحتى البحث باللغة العربية لم يعطي ولانتيجة واحدة وبدأت أغير كلمات البحث وأضيف وأحذف حتى وجدت أحد الطرق والتي سوف أقدمها لكم اليوم وهي لانتحتاج إلى أي برامج قرصنة كل ما نحتاجه ملفان صغيران جدا وحجمهم 50 كيلو بت بس ومن مايكرووسوفت قم بتحميلهم الآن ولنبدأ بعدها أول الخطوات

رابط التحميل تجده على موقع المجلة **www.networkset.net** قم بعمل إعادة أقلاع وبعدها قم بالضغط على زر **F8** لأظهار كل الخيارات المتاحة وقم باختيار **Directory Restore Service Mode**



بعد ظهور شاشة الدخول إدخال على الكمبيوتر من خلال حساب الأدمن وبدون باسورد واذا لم تستطع قم بالاستعانة بسيدي الهايرن وقم بحذف كلمة السر الخاصة بحساب المدير وأدخل إلى الجهاز ومبروك عليك كسر كلمة السر..... لكن مهلا لافتح الدومين وأقوم بتغيير كلمة السر الخاصة بي والمفاجئة ممنوع الأقتراب والمساس بالدومين أبداً وحتى مشاهدة مابدأخله ممنوع !!! لتتابع إذا طريقة تغيير كلمة السر

لنتوجه الآن إلى قرص السي ولنقم بإنشاء ملف جديد وليكن أسمه **recovery** ونضع فيه الملفان الذان قمنا بتحميلهم زائد موجه الأوامر **CMD** والذي سوف تجده داخل ملف **System32** وهذه صورة توضيحية للملفات الثلاث ومكان الملف



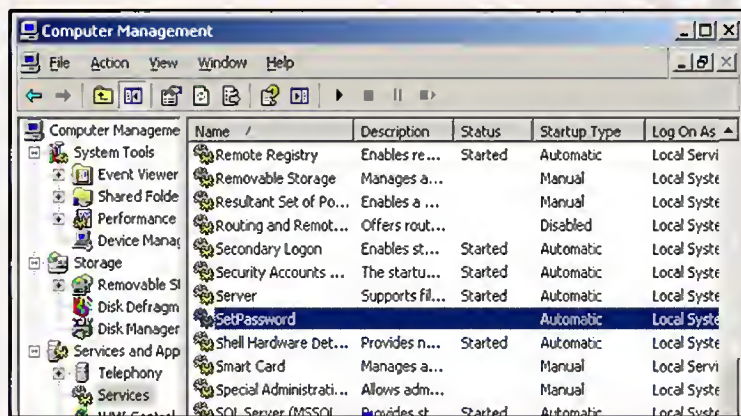
وأخر خطوة نقوم بعمل إعادة أقلاع وننتظر ظهور نافذة الدخول وبعدها ننتظر دقيقة أو أنثان (لكن ليس أقل حتى نضمن أن الخدمة بدأت تعمل وتم تنفيذ الأمر وبعدها قم بأدخال كلمة السر التي قم بأختيارها والتي كانت في هذا الشرح **P@ssw00rd** ومبروك عليك كسر الدومين وتغيير كلمة السر وبقي شيء واحد صغير وهو حذف الخدمة من الجهاز وهي تتم من خلال كتابة الاوامر التالية في موجه الاوامر الذي سوف تجده ينتظرك بعد الدخول إلى جهاز الكمبيوتر

net stop SetPassword
sc delete SetPassword

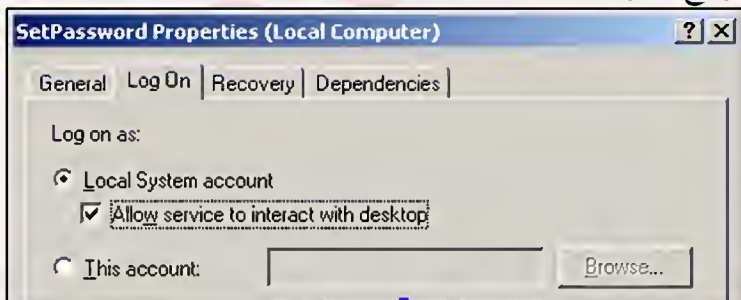
إذا كيف تم الأمر الموضوع بسيط جدا واعتقد أنك قد فهمته أثناء شرح الخطوات والفكرة ببساطة تتم من خلال تنصيب خدمة زائفة على نظام التشغيل والتي تتم من خلال الأداة الأولى وهي **Instrsrv.exe** المسؤولة عن تنصيب وحذف الخدمات **Services** أما الأداة الثانية فهي تسمح لنا بتشغيل بعض التطبيقات كخدمة موجودة في نظام التشغيل وهي طبعاً موجه الاوامر **CMD** الذي قمنا بأضافته في الريبجستري وبعدها قمنا بكتابة الأمر الذي سوف يقوم بتغيير الباسورد لحساب المدير وهو أمر الـ **net user** والفترة التي أنتظرنا فيها بعد إعادة الأقلاع من أجل تشغيل الخدمة الزائفة وتنفيذ أمر التغيير وأنهى الأمر

كلمة أخيرة هذه الطريقة سوف تفتح أمامك الكثير من الأشياء المفيدة والتي يمكن تطبيقها على نظام التشغيل بغض النظر عن موضوع إستعادة كلمة السر بس أنت فكر فيها !!! وأخيراً أتمنى استخدام هذه الطريقة في الخير وحل المشاكل وليس في طريق إيذاء الآخرين وخليك حريص مع الأشخاص الذين يعملون معك في الفترة الأولى

والخطوة قبل الأخيرة توجه إلى إدارة الكمبيوتر **Computer Management** وبعدها إلى **Services** وإبحث عن الخدمة الجديدة التي قمنا بأضافتها وهي بأسم **SetPassword**

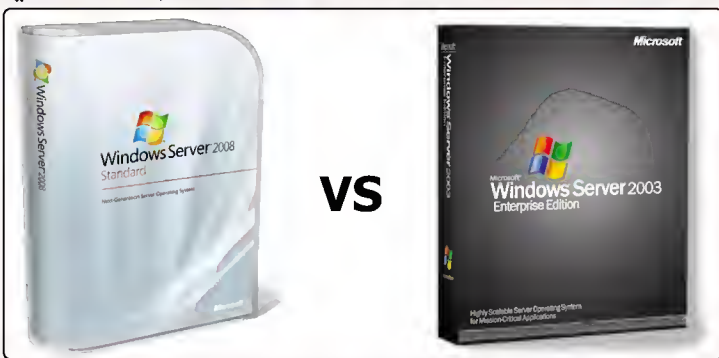


نقوم بالضغط عليها مرتين وتوجه إلى **Log on** ونقوم بالتأشير على المربع الصغير الموضح بالصورة



أهم الاختلافات بين ويندوز 2003 وويندوز 2008

بقلم: ياسر رمزي



ايضا تم استبدال الـ **RIS** بـ **WDS Windows Deployment Services** فاصبحت عملية انزال نسخة ويندوز على مجموعة اجهزة تلقائيا اكثر سهوله و اكثر تحكما خاصة بعد استخدام **Windows Imaging Format** كذلك تم اضافة الـ **Failover Clustering** كخاصية تسمح جعل مجموعة من الخوادم تعمل معا وتعمل بدل بعضها في حالة فشل احدهم ايضا مع نسخة الويندوز سيرفر **2008** الـ **R2** اصبح لدينا برنامج بديل لـ **MICROSOFT VIRTUAL SERVER** نسيمه **HYPER-V** لبدء ميكروسوفت مرحلة جديده في عالم الـ **virtualization** اخيرا دعونا نتحدث عن احد الاختلافات الهامه في نسخ ويندوز المعتاده ففي **2008** يوجد لدينا اربع نسخ تماما مثل **2003** وهي:

- STANDRAD**
- ENTERPRISE**
- DATACENTER**
- WEB**

ولكن الان في **2008** لدينا نسخة مميزة نسيمها **SERVER CORE** تأتي مع النسخ الثلاثه الاولى حيث يمكن تنزيل نسخة من الويندوز بدون شاشة **DESKTOP** المعتاده بل تم استبدالها بالـ **CMD** لتصبح نسخة ويندوز تعمل من سطر الاوامر بدون واجهة رسومية ولكن هذا لا يمنع ان نشغل بعض التطبيقات بواجهتها الرسومية كالـ **notepad** ففي الحقيقه مازال الـ **explorer** يعمل في خلفية النظام

جاءت نسخة **2008** لتشمل مجموعه كبيره من التحسينات على مكونات وينوز سيرفر **2003** من مكونات تخص النظام الي البرامج التي تأتي معه فمثلا لدينا تغيير جوهري في اسلوب عمل الـ **domain controller** حيث أصبح لدينا نوعين منه النوع الاول نسيمه **writeable domain controller** وهو نفسه المتعارف عليه في النسخه الاقدم وينوز **2003** حيث يتم ابلاغ الدليل النشط **active directory** فيه بأي تعديلات او اضافات لـ **objects** النوع الثاني نسيمه **RODC read only domain controller** وهذا يعني ان نسخة الدليل النشط فيه لن تسجل اي **object** جديد اي نسخة لتوثيق دخول المستخدمين و غيرها فقط وغالبا ما يتم وضع **RODC** في **sites** بعيدة تمثل فروع الشركه حيث لا يوجد مدراء يمكنهم ادارة **domain controller** بشكل موثوق فيه لدينا ايضا الان خمس نسخ من الـ **active directory** تمثل خمس **server roles** جديده هي:

- AD CS Active Directory Certificate Service**
- AD DS Active Directory Domain Service**
- AD FS Active Directory Federation Services**
- AD LDS Active Directory Lightweight Directory Services**
- AD RMS Active Directory Rights Management Services**

ولكن النسخه **AD DS** هي التي تماثل الـ **ROLE** الذي كنا نسيمه **domain controller (active directory)** في نسخة الـ **2003** لدينا ايضا مجموعه من التحسينات جاءت مع برنامج الـ **backup** الذي أصبح يستلزم انزاله من الاسطوانه ايضا تم تحسين الـ **quota** واصبحت تطبق على الـ **folders** وليس الـ **volumes** فقط تم تحسين برنامج الـ **firewall** و اضافة الـ **network access protection** بشكل اكثر فعاله

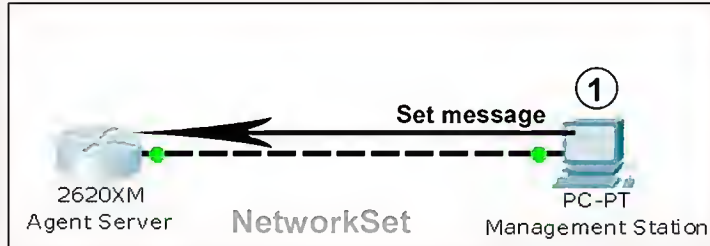
كل ماتحتاج أن تعرفه

حول بروتوكول

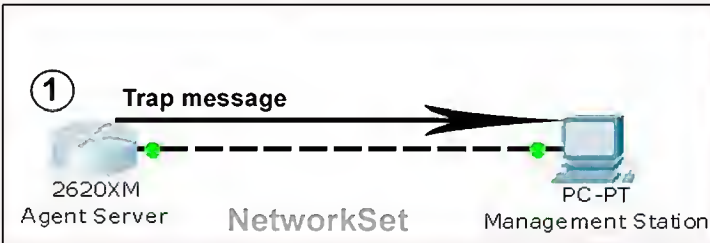
SNMP

أعداد: أيمن النعيمي

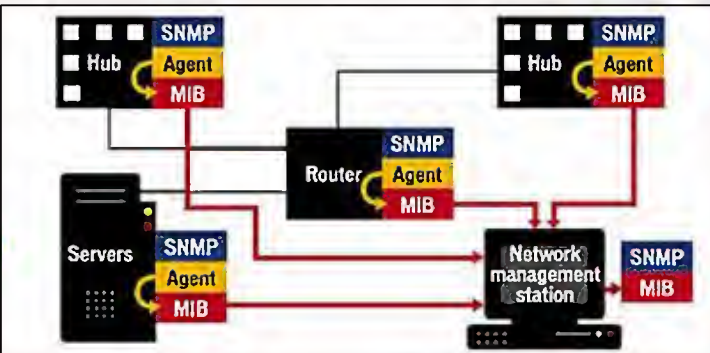
رسالة ال Set ترسل من قبل العميل لكي يطلب من ال Agent ما لشيء يتم تحديده في حال حدوث أي تغيير على السيرفر تغيير قيمة



رسالة ال Trap ترسل من قبل ال Agent في حال حدوث شيء ما في لجهاز المراقب مثلا توقف بورت عن العمل (Link Down/Up) وهو في هذه الحالة يرسلها على البورت 162 بينما باقي الرسائل ترسل على البورت 161



والصورة القادمة تشرح لنا كيف يعمل ال SNMP من الداخل



ويتضح لنا أن ال Agent يأخذ الطلب من العميل ويضعه في MIB Management Information Base وبدوره يقوم ال MIB بأرسال المعلومات المطلوبة الى العميل ولا SNMP ثلاث إصدارات مختلفة

SNMPv1

SNMPv2

SNMPv3

في الإصدار الثاني تم استبدال ال Get-Next بـ ال Get-Bulk التي تستطيع تحمل معلومات أكبر بالإضافة لبعض أمور الأمن والسيكورتية والعديد من مميزات المراقبة وقد تم إصداره عام 1997 أما الإصدار الثالث وهو المستخدم في وقتنا الحالي منذ عام 2004 فقد تم إضافة

بعض الأمور مثل

Authentication

Privacy

access control

وبالنسبة للبرامج المستخدمة فهي كثيرة جدا ولكل برنامج له مميزاته الخاصة

في ظل الأنفتاح الكبير على الانترنت وعلى الشبكات وزيادة نسبة الأجهزة التي تقوم بعملية إدارة الشبكات مثل الروترات والسويتشات وزيادة فعاليتها يوم بعد يوم وحتى يستطيع مهندسي الشبكات مراقبة أجهزتهم وطريقة أدائها فكان لا بد لهم من إيجاد بروتوكول خاص للمراقبة عن بعد بحيث يعطيهم بيانات دائمة لكفاءة عمل الأجهزة على الشبكة وبما فيها كفاءة عمل المعالج والرامات وكمية نقل البيانات ضمن الشبكة والكثير من خصائص المراقبة الهامة

مراحل تطوير البروتوكول

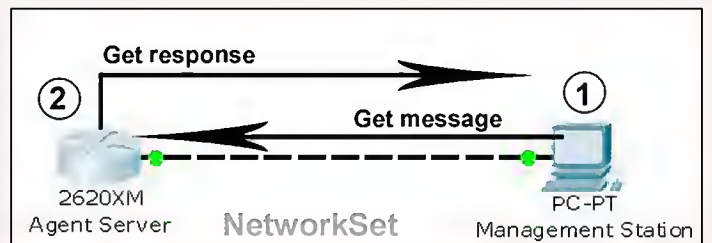
تم البدء في تطوير بروتوكول ال SNMP عام 1988 ليقيم بعملية المراقبة وهو بروتوكول مطور من بروتوكول آخر تم تطويره عام 1987 اسمه CGMP أو Simple Gateway Management Protocol وجاء بعده بروتوكول آخر ظن الجميع انه سوف يحل مكان SNMP وهو CMIP secure Common Management Information Protocol لكن الأخير لم يدوم كثيرا كون ال SNMP أثبتت فعاليتها بشكل أقوى على الساحة كونه يعمل على نطاقات واسعة وقابل للعمل مع جميع أنواع مكونات الشبكة (Network component)

وفي الحقيقة بروتوكول ال SNMP يقسم الى قسمين: القسم الأول ويدعى ال Agent او السيرفر وهو هنا الجهاز المراد مراقبته مثل الروتر، السويتش، الطابعة الخ القسم الثاني Network Management Station (NMS) أو العميل وهو لجهاز الذي سوف يستلم البيانات من ال Agent

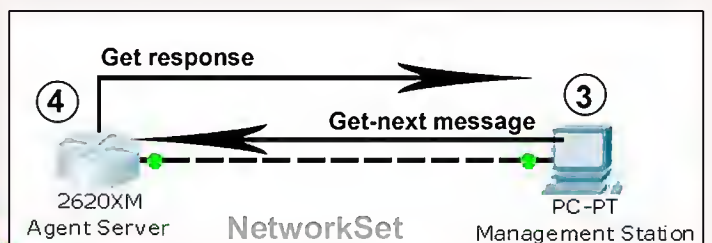
كيف يعمل ال SNMP ؟

لنتفق أولا على الأشياء الأساسية التي يجب ان نعرفها وهي أن هذا البروتوكول هو أحد بروتوكولات الطبقة السابعة Application Layer ويستخدم ال UDP/IP للأرسال ومن خلال البورت 161 و162 وهو يستخدم خمس أنواع من الرسائل للتواصل بين السيرفر والعميل وهي GET, GET-NEXT, GET-RESPONSE, SET, and TRAP

فعندما يريد العميل ان يبدأ المراقبة يقوم بأرسال ال Get message الى ال Agent وهو بدوره يرسل المطلوب على شكل ال Get-Response وكما نرى من الصورة القادمة



أما بالنسبة للرسالة ال Get-Next فهي عندما يريد أن يتابع عملية المراقبة ويرغب في الحصول على المزيد من المتغيرات



لاحتار بعد الآن في اختيار الكبل المناسب مع تقنية الـ Auto-MDIX !

السويتش وبغض النظر اخترت Straight or cross over، ويتطلب أعدادها شيئا مهماً أن تكون حالة الـ Duplex والـ Speed على الوضع Auto هذه التقنية مدعومة من بعض سويتشات سيسكو وهي بالترتيب 2940, 2970, 3750 وطريقة الأعداد بسيطة جدا

```
Switch# configure terminal
Switch(config)# interface fastethernet 0/1
Switch(config-if)# speed auto
Switch(config-if)# duplex auto
Switch(config-if)# mdix auto
Switch(config-if)# end
```

وبحسب ما قرأت على موقع جونيور أن هذه التقنية مدعومة في أغلب السويتشات الخاصة بجونيور وأخيراً أحب أن أضيف أن هذه التقنية ليست حديثة وعمرها حوالي العشر سنوات

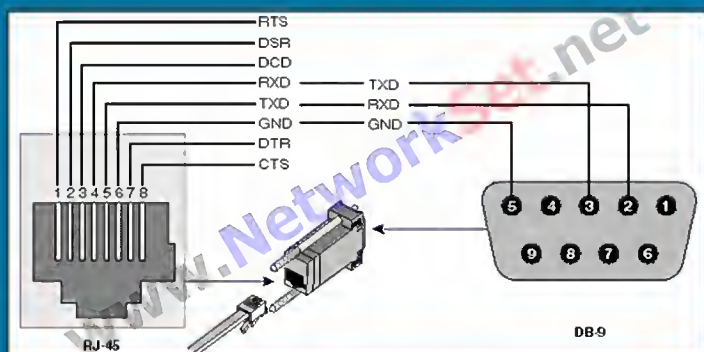
Auto-MDIX هي أحد التقنيات المطورة من قبل شركة HP والتي قام بتطويرها Dan Dove و Bruce Melvin تسمح لنا هذه التقنية بوضع أي كبل كان نوعه Straight-Through أو Cross Over في السويتش بغض النظر كان الربط مع هوب أو روتر أو جهاز كمبيوتر لأن البورت بشكل أوتوماتيكي سوف يختار ماهو الكبل الذي يناسبه، فكما هو معروف أن للأجهزة الموجودة على الشبكة قسمين رئيسيين MDI وهي تشمل المنافذ الموجودة على جهاز الكمبيوتر NIC والمنافذ الخاصة بالروتر MDIX وهي تشمل المنافذ الموجودة على السويتش أو الهوب أو البريدج

فندما نريد أن نربط جهاز MDI مع جهاز MDIX نستخدم كابل من نوع Straight وعندما نريد أن نربط MDI مع MDI نستخدم Cross Over وعلى ما يبدو أن هذه القصة قد سببت بعض المشاكل لي Melvin عندما كان يبحث عن كابل كروس أوفر في مخبره ولم يجده

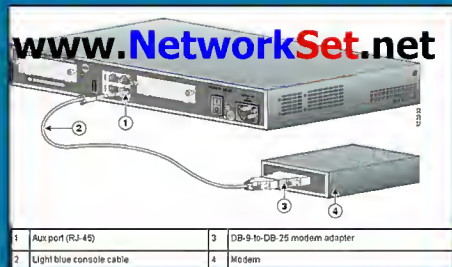
فطلب من Dove أن يجد له حلاً وبالفعل قام Dove بتطوير تقنية تتعرف على أسلاك التوصيل المسؤولة عن عملية إرسال واستقبال الداتا وبشكل أوتوماتيكي تتأقلم مع

أهم الاختلافات بين منفذي الـ Console Port و Auxiliary Port

وهذه صورة توضيحية لطريقة ربط الأسلاك ببعضها

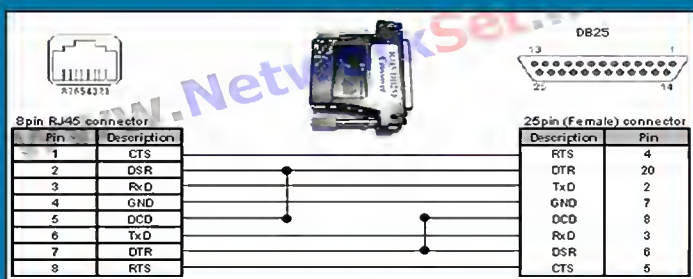


بالنسبة للـ Auxiliary Port هذه صورة توضح كيفية ربطه مع مودم خارجي وتبين نوع الكوابل والمحولات المطلوبة وهو بالعادة يتصل مع المودم من خلال DB25 أو من خلال Rollover Cable



1 Aux port (RJ-45) 2 Light blue console cable 3 DB-9 to DB-25 modem adapter 4 Modem

وهذه صورة توضيحية لتوزيع الأسلاك بين RJ-45 و DB25

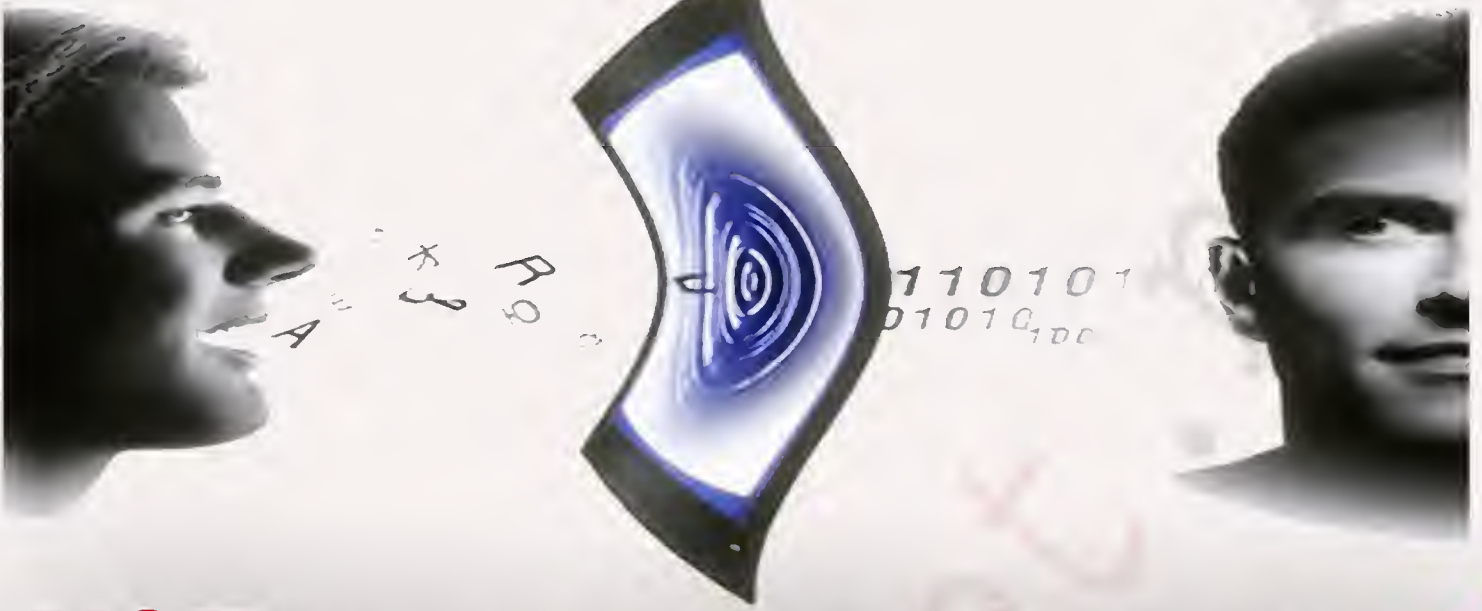


كما هو معروف أن أغلب الأجهزة المستخدمة في الشبكة سويتش كانت أو روتر تحوي مخرجان واحد للـ Console وواحد للـ Auxiliary وكلا المنافذ يستخدمان من أجل أعداد والتحكم في الروتر لكن السؤال الآن متى أستخدم كل واحد منهم؟ لننتقل أنك كنت بعيد عن مكان وجود الجهاز وحدثت مشكلة في الروتر ويتطلب منك الدخول إلى الروتر وأصلاح الخلل وطبعاً لا يتم إلا من خلال الـ Console أو Auxiliary وطبعاً عن طريق الكونسول بورت صعب لأنه يتطلب أن تكون بجانب الجهاز لذا تم إيجاد الـ Auxiliary Port الذي يتيح لك التحكم بالروتر من بعيد عن طريق ربط المنفذ بمودم والذي بدوره يتصل مع الإنترنت ويسمح لك بالولوج إلى الجهاز وأجراء التعديلات المناسبة وهو

الفرق الأول بين الاثنين وهو إمكانية التحكم بالجهاز عن بعد وقد يسأل البعض لماذا لا أتحكم بالجهاز عن طريق التلنت وطبعاً الجواب غير ممكن لأن الشبكة عبارة عن شبكة داخلية لشركة ما وليست مرتبطة مع الإنترنت وهي لاتملك أيبيات حقيقية الفرق الثاني وهو أن الـ Auxiliary port يعتمد على خاصية الـ Flow Control بينما الكونسول غير مزود بمثل هذه الخاصية وأقول للذين لا يعلمون عن هذه الخاصية بأنه تقوم بتقطيع البيانات إلى أجزاء صغيرة ويتم إرسالها وهي طبعاً تراقب البافر الموجود في الجهاز المستقبل في حال امتلأ وطبعاً هذه الخاصية تعطيني دقة وأمان في نقل المعلومات من وإلى الجهاز وبمعنى آخر التأكد من وصول المعلومات بشكل صحيح الفرق الثالث هو السرعة ففي حال كان المودم يدعم سرعات كبيرة فهذا يعطيني سرعة أكبر من الكونسول بورت والسبب أن سرعة الكونسول بورت تكون محدودة بعكس المودم الذي تزيد سرعته بحسب سرعة الإنترنت

بالنسبة لطريقة التوصيل فسوف أشرحها بالصور التالية ونبدأ مع صورة للكابل المخصص للكونسول وهو عبارة عن RJ-45 to DB9، والصورة لنا من الصورة ان بإمكاننا صنع كابل مباشر بينهم أو استخدام تحويلية Adapter تقوم بتحويل المنفذ من RJ-45 إلى DB9





كيف تقوم بتأسيس شبكة فويس من الصفر (VOIP)

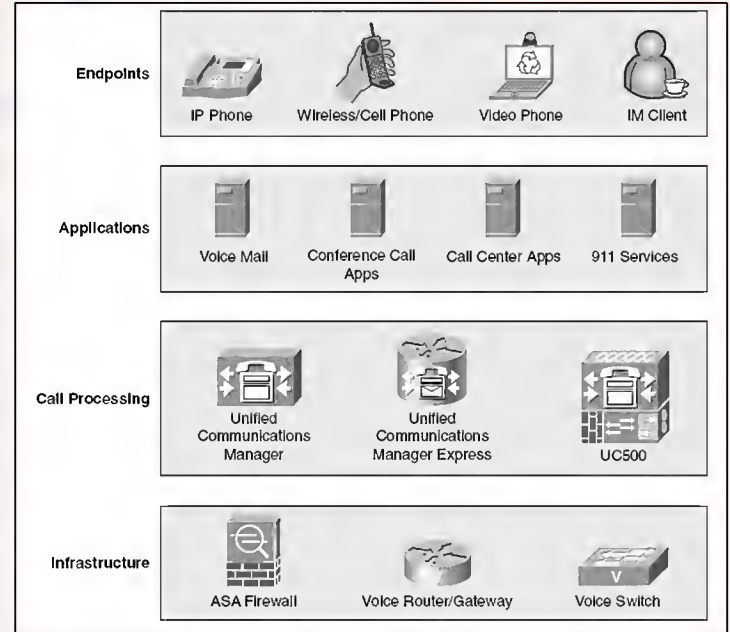
بقلم أحمد الشحات

أستكمال للسلسلة التي بدأناها في بناء شبكة فويس من الصفر والتي كانت مقدمة حول هذه الخدمة و توضيح فوائدها ومميزاته اما اليوم فسنتكلم عن مكونات الشبكة الجديدة التي سانتقل اليها وبالطبع ستكون هناك اجهزة جديدة فى الشبكة لم اراها من قبل وستكون هناك اجهزة استخدمتها بالفعل فى خلال عملي كمهندس شبكات وهناك اجهزة مزدوجة الاستخدام مع شبكة الهاتف ومع شبكة الداتا

مكونات شبكة الفويس

ويوجد منها نوعان :

Analog Gateways وتحتوي على منافذ ال **FXS** الذي يوصل بهاتف عادي أو فاكس
و ال **FXO** الذي يوصل بخط التليفون القادم من **PSTN**
Digital Gateways وتحتوي على منافذ ال **1T/1E**
ومن الروتات المستخدمة في سيسكو حديثاً **Voice Gateway** : **2800** , **3500** , **6500**



نلاحظ من خلال هذه الصورة أن الأجهزة المستخدمة فى شبكة الفويس تنقسم الى عدة طبقات كما هو الحال فى شبكة الداتا ايضا ولكن طبعا مع اختلاف المسميات واختلاف الاجهزة المستخدمة فى كل طبقة وهذه الطبقات هي

- 1-INFRASTRUCTURE
- 2-CALL PROCESSING
- 3-APPLICATIONS
- 4-END POINTS

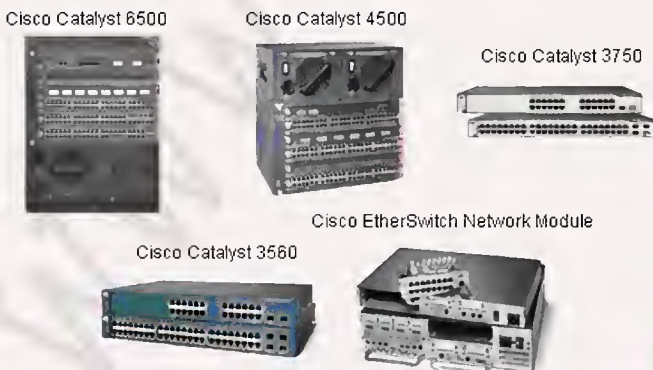
هذه الطبقات تخدم بعضها من أجل بناء شبكة ال **Voice** ، وسوف نتعرف على أهم الأجهزة المستخدمة في كل طبقة من هذه الطبقات في عالم الفويس

1- Voice Router/Gateway : هو راوتر يستخدم ليكون وسيلة ربط بين الشبكات المختلفة مثل الربط بين شبكة الفويس وشبكة ال **PSTN** أو بين شبكة الفويس وشبكة أخرى عبر ال **WAN** ، ويقوم بتحويل البايت إلى شكل يلائم الشبكة المنقول إليها المكالمات وبالتالي سيكون قادر على عملية **compression** و **decompression** و **Control** و **Signaling** و **Call Routing** ، كما أنه يعتبر وسيلة لتوصيل **Analog device** مثل التليفون العادي والفاكس وال **PBX**



Cisco 6500 Series Cisco 2800 Series

Voice Switch-2 : أيضا هو سويتش يدعم العديد من الوظائف التي قد تحتاجها في عالم الفويس وأهمها **Quality of Service (QOS)** و خاصية **Power Over Ethernet (POE)** والتي تمكن السويتش من تزويد الهاتف بالطاقة اللازمة بدلا من توصيل الهاتف بتوصيلة كهرباء خاصة به . وأيضا تدعمه ال **Voice Vlan** والتي تمكنني من جعل الهاتف والكمبيوتر على نفس البورت في السويتش ولكن كل واحد منهم في **Vlan** مختلفة من أجل حماية ال **Voice** وإعطاء أولوية للفويس عن الداتا. وهذه أشهر الأنواع المستخدمة في عالم الفويس



Internet low bandwidth codec (iLBC) at 15.2 kbps, and G.722 wideband audio codec at 64 kbps
LAN : هل التليفون به port لتوصيل الحاسب به وما سرعته
Phone buttons : وتختلف من جهاز لآخر
Speakerphone and headset support : الأغلبية تدعمها
Number of lines : من 1 إلى 8 خطوط أو 24 خط ، أو إمكانية التوسعة وإضافة 28 خط
Other features : مثل video, WiFi و external microphones
 وبناء على الخصائص السابقة يتم تقسيم التليفونات إلى ثلاثة أقسام :

القسم الأول : Entry Level Cisco IP Phones

منها تليفونات 7906 و 7911

Message waiting indication - بها لها خط واحد - **tor**

يختلف 7911 عن 7906 أن الأول به منفذ للحاسب الآلي أما 7906 فلا يحتوي على منفذ للحاسب

يتيح لك إجراء مكالمات واستقبالها ووضع مكالمات في الانتظار وتحويلها والوصول إلى بيانات الشبكة وتطبيقات XML والخدمات المستندة إلى الويب

القسم الثاني : Midrange Cisco IP Phones

مثل 7940, 7961, 7941, 7942, 7941, 7942

dual line

full xml application

built in switch - له منفذ للحاسب

الرمز GE أي سرعة البورت gigabit

القسم الثالث : High-End Cisco IP Phones

مثل 7945 و 7965 وهو نفس خصائص 7942 إلا أنه يتميز بالدقة العالية جدا

Other Cisco IP Phones

Cisco Unified IP Phone 7985 : به كاميرا من أجل تدعيم الفيديو - خط واحد - شاشة LCD - به بورت شبكة فقط

Cisco Unified IP Conference Station 7936

من أجل المؤتمرات الصوتية - يدعم الميكروفونات الخارجية

Call Manager-3 أو Call Agent و آخر اسم أطلقته سيسكو عليه هو Cisco Unified Communication Manager (CUCM)

وهو عقل الشبكة بل قلبها فمن خلاله يتم التحكم في كل شيء ، فهو يزود التليفون (IP PHONE) بالحرارة (Dial Tone) ويقوم بتجميع الأرقام المطلوبة من المستخدم وإجراء المكالمات والتحكم في كل شيء .

وهو عبارة عن سيرفر له إمكانيات خاصة وكانت شركة IBM و HP هم المستحوذين على التصنيع وقد أوقفت سيسكو التعامل مع HP وأصبح لها سيرفرها الخاص . ومن أمثلة على هذه السيرفرات



mcs 7816 ويدعم من 300 إلى 500 تليفون
 mcs 7825 ويدعم حتى 1000 تليفون
 mcs 7835 ويدعم حتى 2500 تليفون
 Mcs 7845 ويدعم حتى 7500 تليفون

ولقد مر الكول مانجر بعدة إصدارات فمنها ما هو يعمل في بيئة الويندوز مثل 3.X و 4.X ومنها ما يعمل في بيئة linux مثل الإصدار 5, 6, 7

ويطلق على الأخير **appliance model**

بالنسبة للإصدار 4 وهو المتبقي حالياً من الإصدارات القديمة وفي طريقه إلى الزوال:

فهو يعمل تحت ويندوز 2000 أو 2003 ويعتمد في قاعدة البيانات على SQL 2000 كما يعتمد على **Domain Controller** كما تستطيع استخدام نظام التشغيل (ويندوز) بشكل كامل

أما بالنسبة للإصدارات 5, 6, 7 فإنها

مبني على نظام التشغيل **Redhat linux enterprise**

ولن ترى نظام التشغيل linux ولن تعمل عليه

يعتمد على قواعد البيانات **IBM Informix Dynamic Server**

و **Cisco Security Agent**

ملحوظة : يوجد ما يسمى ب **Call Manager Express** وهو راوتر يدعم الفويس وعليه **IOS** خاص بذلك ولكنه يُستخدم في الشبكات الصغيرة أو يُستخدم في فرع بعيد للشبكة به عدد قليل من التليفونات لتوفير التكاليف ، وحسب إمكانيات الراوتر تختلف عدد التليفونات التي يدعمها

Cisco Unity-4 : هو سيرفر يستخدم من أجل التعامل مع جميع أنواع الرسائل وجعلها في صندوق واحد سواء كانت **fax message** أو **voice mail** أو **email** وهو يمكنك من سماع الإيميل من خلال التليفون ، ويستطيع الرد على المكالمات .

Cisco Unified Contact Center-5 : وهو عبارة عن سوفتوير يعمل على سيرفر من أجل توزيع المكالمات داخل الشركة **call center**

end point-6 : يوجد العديد من أجهزة ال **end point** والتي يمكن استخدامها مع ال **CUCM** سواء كانت هذه الأجهزة من سيسكو أو من شركات أخرى **third party** وهذه الأجهزة تشمل ال **IP phone** و **analog gateways** و **video endpoints**

هناك ثلاث بروتوكولات للتواصل بين هذه الأجهزة وال **CUCM** : وهي **SCCP** و **SIP** و **H.323**

بالنسبة لل **SCCP** فهو بروتوكول خاص بأجهزة سيسكو فقط ، إلا أنه توجد بعض الشركات **licensed SCCP** لها (**P blueI, Sony, Tandberg, and VTGO**)

وبالتالي تقدم العديد من المميزات والخصائص التي تقدمها أجهزة سيسكو .

بالنسبة لل **SIP** و **H.323** مع أجهزة الشركات الأخرى غير سيسكو فإنها مع ال **CUCM** تدعم الأشياء الرئيسية من أجل الاتصال ولا تدعم كل المميزات التي تدعمها أجهزة سيسكو .

بالنسبة لأجهزة سيسكو التي تدعم ال **SIP** فإن المميزات والخدمات التي تقدمها تختلف من جهاز لآخر

ويوجد تصنيفان من أجهزة سيسكو التي تدعم ال **SIP**

Type A phones: IP Phones: 7905, 7912, 7940, and 7960.

Type B phones: IP Phones: 7906, 7911, 7931, 7941, 7942, 7945, 7961, 7962, 7965, 7970, 7971, and 7975.

أجهزة ال **Type B** تعطي وتقدم خدمات أكثر من التي تقدمها أجهزة ال **Type A**

Cisco IP Phone Models

تختلف التليفونات عن بعضها طبقاً لمواصفات عديدة منها

Screen : من حيث مساحتها - اللون - الدقة - هل تعمل باللمس أم لا ؟

Codec support : ما هو نوع ال **codec** الذي يدعمه هل هو **G.729, G.711, iLBC, wideband**

كل تليفونات سيسكو تدعم ال **G.729, G.711, iLBC** والكثير منها يدعم **G.729, G.711, iLBC** , وجميع ال **Type B** تدعم هذا ال **Codec**



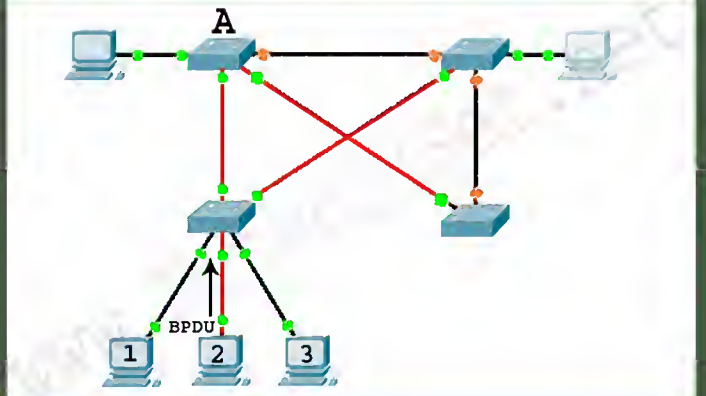
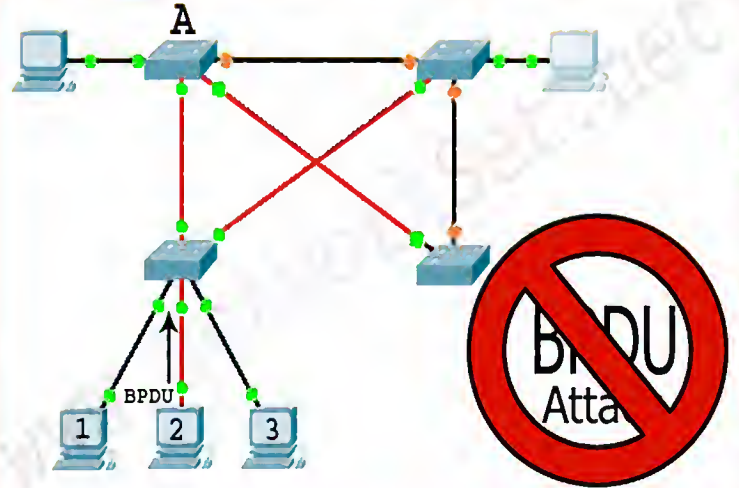
قسم أمن وهماية الشبكات

هذا القسم سوف يتم عرض فيه كل الامور الواجب عملها في الشبكة بهدف التخفيف من نسبة القرصنة التي تحدث على الشبكة وأرجو منك أن تدقق على كلمة تخفيف لان النظرية العامة تقول لا يوجد جهاز آمني خالي من الثغرات مهم كانت قوته!

هجوم الـ STP manipulation وطريقة التصدي له

وقدنة عن بروتوكول الـ Spanning Tree

كما هو معروف عند الجميع أن بروتوكول الـ STP يلعب دورا كبيرا في الشبكة في منع ما يعرف بي الـ loop أو Broad-cast Storm ويتم ذلك عن طريق أنتخاب سويتش واحد ليكون Root Bridge ويتم الأختيار حسب أقل Bridge ID موجود على الشبكة وبعدها يتم أختيار البورتات التي يجب أن تعمل أو تتوقف أعتيادا على الـ Cost أو التكلفة للوصول للـ Root Bridge وكل هذه الامور تتم عن طريق ما يعرف بي BPDUs وطبعا هذا الكلام معروف عند الجميع



وسوف نلاحظ ان كل شيء قد تغيير وأصبح كل الترافيك الذي يعبر عبر الشبكة يمر عبر الشخص المهاجم وبالتالي أصبح عندنا الهجوم الذي يعرف بي MITM أو Man In The Middle

كيف أحمي شبكتي من هذا النوع من الهجوم ؟

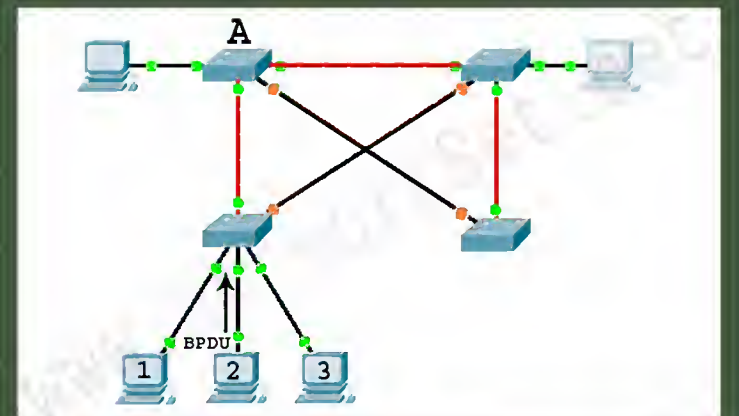
سيسكو تقترح عليك 3-طرق للحماية من هذا الهجوم الأولى

BPDUs Guard خاصية تخبر فيها البورت أن لا يستقبل أي نوع من رسائل الـ BPDUs وفي حال أستلام البورت لأي BPDUs سوف يقوم بتحويل حالة البورت إلى errdisable أي سوف يتم إغلاق البورت بشكل كامل وطريقة الأعداد تتم على الشكل التالي :
نتوجه أولا إلى البورت الغير آمن وأقصد فيه أي بورت موصول مع جهاز كمبيوتر أو أي شيء غير السويتش وبعدها أقوم بكتابة الأمر التالي

`Switch(config-if)#spanning-tree bpduguard enable`

كيف يتم هذا النوع من الهجوم ؟

الهجوم كغيره فكرته بسيطة وتأثيره كبير جدا وهو يتم عن طريق إرسال BPDUs مزور يخبر فيه المهاجم السويتش الذي يرتبط معه بأنه يملك أقل Bridge ID على الشبكة وبانه يجب ان يكون هو الـ Root Bridge وبالتالي سوف تتم إعادة توزيع البورت على كل السويتشات وهذه بعض الصور لتبسيط الموضوع
الصورة الاولى نرى فيها التوزيع الطبيعي للشبكة ونرى أيضا أن السويتش A هو الـ Root Bridge على الشبكة والخطوط الحمراء خاصة بي الـ STP ونرى أن المهاجم الموجود على الجهاز رقم 2 يقوم بأرسال BPDUs مزور إلى السويتش



الخطوط الحمراء تدل على أن اللينك في حالة Forwarding بينما الخطوط السوداء تدل على أن اللينك في حالة Blocking وفي الصورة الثانية سوف نشاهد ماذا سوف يحدث بعد أن يقوم المهاجم بتغيير المخطط

Switch(config-if)#spanning-tree bpduguard enable

وإذا أردنا نقوم أن نقوم بتفعيل هذه الخاصية على كل البورتات التي هي في حالة PortFast أكتب الأمر التالي في الـ Config mode

Switch(config)#spanning-tree portfast bpduguard default

كلمة أخيرة أحب أن أضيفها وهي يجب الحذر من هذا النوع من الهجمات بسبب قدرته على تخريب الشبكة بشكل كامل بالإضافة إلى إمكانية المهاجم في التنصت على كل ما يجري في الشبكة وأقصد بهذا ليس فقط السويتش الذي ينتمي إليه المهاجم بل كل السويتشات الموجودة على الشبكة

وإذا أردت أن تقوم بتفعيل هذه الخاصية على كل البورتات التي تكون في حالة PortFast أكتب الأمر التالي في الـ Config mode

Switch(config)#spanning-tree portfast bpduguard default

BPDU Root وهي الطريقة الثانية لحماية الشبكة من هذا النوع من الهجوم وفيه أخبر السويتش بأن هذه البورت لن يكون أبداً Root Bridge وطبعاً هذا الأمر يفيد في صد الهجوم ويمكن أيضاً الاستفادة منه في حال أردنا أن لا يكون السويتش الموصول مع الطرف الآخر أن يكون Root للشبكة وتتم من خلال هذا الأمر

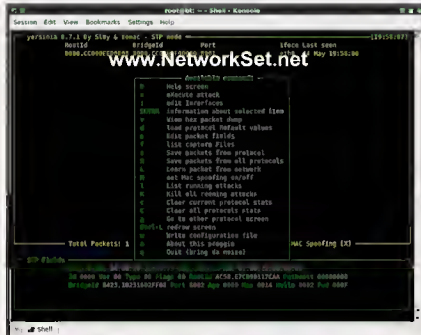
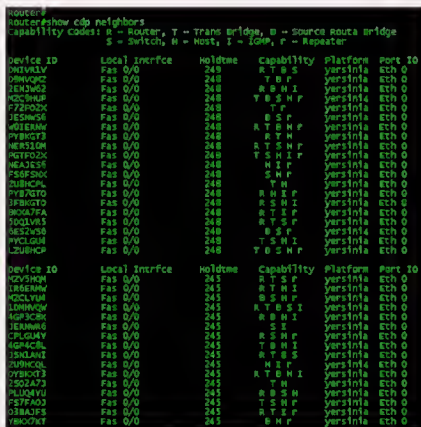
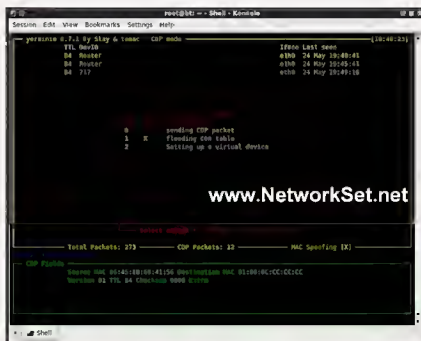
Switch(config-if)#spanning-tree guard root

BPDU Filtering هذه الخاصية هي نفس الخاصية الأولى تماماً والفرق الوحيد هو أن هذه الخاصية تتيح لك أن تحدد ماذا تريد للبورت أن يفعل في حال أستلم BPDU بعكس الـ BPDU Guard الذي سوف يقوم بإغلاق البورت بشكل مباشر وطريقة الأعداد هي كالتالي:

على البورت الغير آمن نقوم بتنفيذ الأمر التالي

أداة Yersinia الأفضل في اكتشاف ثغرات السويتش

أعداد أيمن النعيمي



بعد تحديد البروتوكول المراد فحصه نضغط على حرف X لبدء الهجوم على السويتش وطبعاً لكل نوع من البروتوكولات هناك عدة طرق لأخترافه لذا سوف نقوم بتجربة أحد البروتوكولات وهو CDP الخاص بـ سيسكو والمسؤول عن عملية مشاركة المعلومات الخاصة بالأجهزة المربوطة معه لذا سوف أقوم أولاً بالضغط على F1 وبعدها أضغط على حرف X لتظهر لي هذه النافذة والتي منها:

سوف أختار نوع الهجوم المراد عمله: وكما يتضح يوجد لهذا البروتوكول 3 أنواع من الهجوم الأول من أجل إرسال فريم واحد عشوائي على شكل CDP Frame والتي بدورها سوف تتسجل على السويتش المرتبط مع الجهاز ولو قمنا باختيار رقم واحد سوف أقوم بعمل فلوود للسويتش من خلال إرسال آلاف الطلبات من CDP Frame العشوائية ولو توجهنا إلى السويتش سوف نجد أن القائمة قد امتلأت بالآلاف التسجيلات.

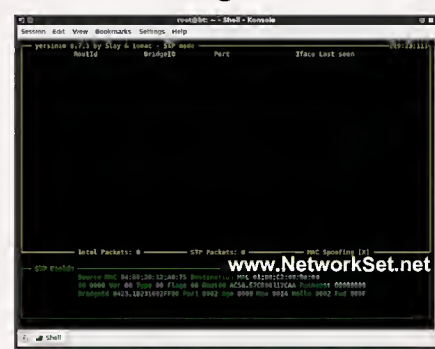
الرقم اثنان يمكننا من عمل جهاز وهمي نقوم نحن باختياره من خلال التعديل على الفريم وللحصول على بعض المساعدة من البرنامج أضغط على حرف h لتحصل على كل إمكانيات الأداة وهي موضحة بالصورة التالية:

شيء واحد أحب أن أؤنوه إليه وهو الحرف e الذي يسمح لنا بالتعديل على الفريم الذي سوف يتم إرساله إلى السويتش وهو موضح في أسفل الأداة

أخيراً أحب أن أقول أن هذه الأداة تعد من الأدوات الخاصة باختبار أمان الشبكات والبروتوكولات المستخدمة فيها لذلك أرجو منك أن لاتستخدمها في غير هذه الأمور

Yersinia وهي أداة خاصة بالشبكات تمكننا من اكتشاف الثغرات ونقاط الضعف الموجودة في الشبكة والأنظمة المستخدمة من خلال فحص وتحليل عدة بروتوكولات وبالأخص البروتوكولات التي تعمل على الطبقة الثانية Data Link مما يعني أن الأداة تستهدف السويتشات بشكل أساسي وهي تدعم البروتوكولات التالية:

Spanning Tree Protocol (STP)
Cisco Discovery Protocol (CDP)
Dynamic Trunking Protocol (DTP)
Dynamic Host Configuration Protocol (DHCP)
Hot Standby Router Protocol (HSRP)
IEEE 802.1Q
IEEE 802.1X
Inter-Switch Link Protocol (ISL)
VLAN Trunking Protocol (VTP)



واجهة البرنامج

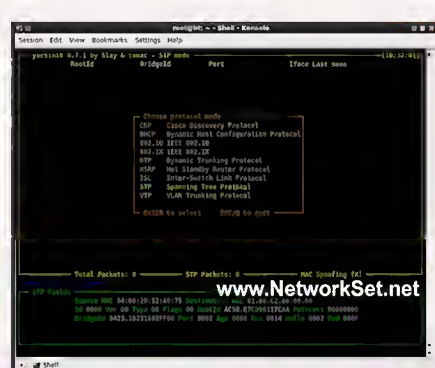
استخدام أداة Yersinia ينحصر في الأنظمة المفتوحة المصدر مثل Linux, OpenBSD, Solaris بالإضافة لدعمها لنظام ماكنتوش 10.4 إلا أن الأداة غير مدعومة في أنظمة ويندوز. سأستخدم بالشرح توزيعه باك تراك حيث الأداة ستكون منضبة وجاهزة للاستخدام بشكل مباشر.

لتشغيل الأداة نتجه إلى سطر الأوامر ونقوم بكتابة:

```
root@bt:~# yersinia -I
```

لتظهر لنا واجهة البرنامج بهذا الشكل:

بعد تشغيل الأداة سوف تبدأ مباشرة بالتنصت على أنواع الفريم الذي يخص البروتوكولات المذكورة ولمشاهدة كل نوع على حدى نستخدم الأزرار الموجودة على لوحة المفاتيح، F1، F2، أو نضغط على حرف F3... F9 لشاهدة قائمة بكل البروتوكولات:



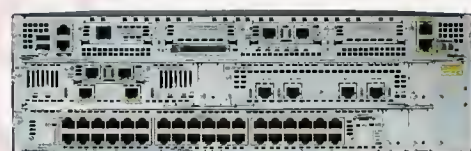
عتاك و محلومات

أعداد عثمان إسماعيل

CISCO SYSTEMS



RAM	512 MB (installed) / 1 GB (max) - DDR SDRAM
Flash memory	128 MB (installed) / 512 MB (max)
Type	Router
MAX Transfer Rate	1 Gbps
Encryption Algorithm	DES, Triple DES, SSL, 128-bit AES, 192-bit AES, 256-bit AES
Supplied OS	Cisco IOS Advanced IP services
Digital Signaling Protocol	Wired
DCP	Ethernet, Fast Ethernet, Gigabit Ethernet
Protocol Remot	SNMP 3, SSH-2
Interfaces	2 x network - Ethernet 10Base-T/100Base-TX/1000Base-T - RJ-45 2 x USB 1 x management - console 1 x network - auxiliary
Firewall protection, hardware compression, hardware encryption, VPN support, MPLS support, content filtering, URL filtering, QoS, Dynamic Multipoint VPN	



CISCO 3845-HSEC/K9

RAM	128 MB
Flash memory	16 MB
Ramer Table of MAC Addr	12K entries
Authentication method	Kerberos, Secure Shell (SSH), RADIUS, TACACS+
Interfaces	management-console RJ-45 2 x network stack device
Connection Type	Half-duplex, full-duplex
Data Rate	100 Mbps
DCP	Ethernet, Fast Ethernet 10Base-T/100Base-TX
Protocol Remote	SNMP1, RMON1, RMON2, SNMP, Telnet, SNMP3
Number of Ports	48 x Ethernet 10Base-T, Ethernet 100Base-TX
Flow control, full duplex, routing, IP-routing, DHCP support, auto-negotiation, ARP support, trunking, load balancing, VLAN support, auto-uplink (auto MDI/MDI-X), IGMP snooping, manageable, IPv6 support	



Catalyst 3750 48TS-E

RAM	256 MB (installed) / 1 GB (max)
Flash memory	64 MB (installed) / 256 MB (max)
Protocol Remote	SNMP 3
Type	Voice / fax module
Interfaces	2 x network - Ethernet 10Base-T/100Base-TX/1000Base-T - RJ-45 2 x USB 1 x management - console 1 x network - auxiliary
Encryption	DES, Triple DES, AES
Supplied OS	Cisco IOS SP services
OS Required	Microsoft Windows 98 Second Edition
DCP	Ethernet, Fast Ethernet, Gigabit Ethernet
Voice Codecs	G.711, G.723.1, G.728, G.729, G.729a, G.729ab, G.726



CISCO 2821-V/K9



Juniper®

NETWORKS

JUNOS Software version tested

JUNOS 10.0

Firewall performance (max)

650 Mbps

IPS performance (NSS 4.2.1)

60 Mbps

AES256+SHA-1 / 3DES+SHA-1 VPN performance

65 Mbps

SRX 100

Maximum concurrent sessions

16 K (512 MB DRAM) / 32 K (1 GB DRAM)

New sessions/second (sustained, TCP, 3-way)

2,000

Maximum security policies

384

Maximum users supported

Unrestricted

Fixed I/O ports

8 x 10/100

CX111 3G Bridge support

Yes

Firewall

- * Network attack detection: Yes
- * DoS and DDos protection: Yes
- * TCP reassembly for fragmented packet protection: Yes
- * Brute force attack mitigation: Yes
- * SYN cookie protection: Yes
- * Zone-based IP spoofing: Yes
- * Malformed packet protection: Yes

Intrusion Prevention System

- * Stateful protocol signatures: Yes
- * Attack detection mechanisms: Stateful signatures, protocol anomaly detection (zero-day coverage), application identification
- * Attack response mechanisms: Drop connection, close connection, session packet log, session summary, email, custom session
- * Attack notification mechanisms: Structured
- * Worm protection: Yes
- * Simplified installation through recommended policies: Yes
- * Trojan protection: Yes



ScreenOS version tested

ScreenOS 6.2

Firewall Perf (Large Packets)

160 Mbps

Firewall Performance (IMIX)

90 Mbps

Firewall Packets Per Second

30,000 PPS

3DES+SHA-1 VPN Perf

40 Mbps

Concurrent VPN Tunnels

25/40*

Max Concurrent Sessions

8,000/16,000*

New Sessions/Second

2,800

Max Security Policies

200

Max Security Zones

8

Max Virtual Routers

3/4*

Max Virtual LANs

10/50*

Fixed I/O

5x10/100

Mini-Physical Interface Module (Mini-PIM) Expansion Slots

2

Physical Interface Module (PIM) Expansion Slots

0

Enhanced PIM (EPIM) Expansion Slots

0

802.11 a/b/g

Optional

Convertible to JUNOS

No

Switch SSG-550M



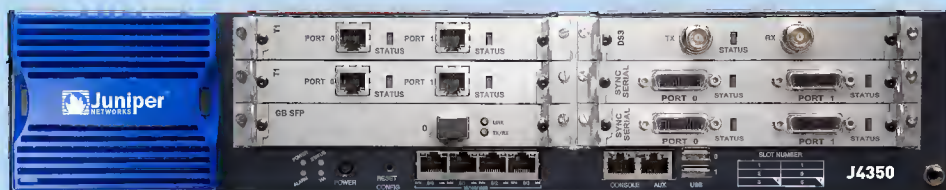
Maximum Performance and Capacity

- * Junos Software Version Support: Junos Software 9.1
- * Firewall Performance (Large Packets): 1.6G
- * Firewall Performance (IMIX): 600 Mbps
- * Firewall and Routing PPS (64 Byte): 225,000 pps
- * 3DES and SHA-1 VPN Performance: 600M
- * Concurrent VPN Tunnels: 512 MB / 1 GB DRAM 256 / 512
- * Maximum Concurrent Sessions: 512 MB / 1 GB DRAM 64 K / 128 K
- * New Sessions/Second: 10,000
- * Maximum Security Policies: 5192 (1 GB DRAM)

Network Connectivity

- * Fixed I/O: 4 x 10/100/1000
- * Maximum PIM Slots: 6
- * Maximum EPIM Slots: 2

Router J4350



Routing, Virtualization, Encapsulations

- * BGP, OSPF, RIP, Static, ECMP: Yes
- * Multicast, PIM SM, SSM, IGMP: Yes
- * Maximum Number of Security Zones: 50
- * Maximum Number of Virtual Routers: Yes
- * Maximum Number of VLANs: 512
- * PPP, FR, MLPP, MLFR, HDLC: Yes

Data Rate

- * EX3200-24P/24T: 88 Gbps
- * EX3200-48P/48T: 136 Gbps

Throughput

- * EX3200-24P/24T: 65 Mpps (wire speed)
- * EX3200-48P/48T: 101 Mpps (wire speed)

10/100/1000BASE-T Port

24 / 48 per platform

100BASE-FX / 1000BASE-X (SFP) Port Densities

4 per switch (via optional four-port GbE uplink module)

10GBASE-X Port Densities

2 per switch (via optional two-port 10GbE uplink module)

Resiliency

External redundant power supply; internal field-replaceable power supply; field-replaceable fan

Power Options

- * AC: 320W, 600W and 930W autosensing; 100-120V / 200-240V
- * DC: 190W; input voltage range 36V-72V; dual input feed

Operating System

JUNOS

QoS Queues / Port

8

Traffic Monitoring

sFlow

MAC Addresses

24,000

Jumbo Frames

9216 Bytes

IPv4 Unicast / Multicast Routes

16,000 / 8,000

Number of VLANs

4,096

Switch EX3200





مصالحات تقنية

Novell IPX : وتعني Internet Network Packet Exchange وهو أحد البروتوكولات التي تم تطويرها من خلال شركة Novel وقد تم بدا التسويق له لأول مرة عام 1980 عندما كانت الشبكات بعدها صغيرة وتعد التكنولوجيا المستخدمة في NetWare بشكل عام مأخوذة من (XNS) Xerox Network Systems وهو نظام شبكات قديم تم عمله لأول مرة عام 1970 ويملك هذا البروتوكول طبقات تختلف عن الطبقات التي عرفناها في OSI

OSI Layer : وتعني Open System Interconnection أو أنظمة الترابط المفتوحة وهو تصميم قامت به منظمة المعايير والمقاييس العالمية ISO وهو يتيح تقسيم الوظائف التي تمر بها الداتا إلى 7 طبقات مختلفة أو Layer ولكل طبقة منها هناك وظيفة أو وظائف محددة تقوم بعملها على الداتا والتي تضمن لنا اكتشاف الأخطاء وتصحيحها في كل طبقة

Physical Layer : أو الطبقة الفيزيائية وهي الطبقة الأولى من الطبقات السبعة OSI Layer وهي مسؤولة عن إرسال واستقبال المعلومات من وإلى الشبكة والقادمة من الطبقات الأعلى منها بالإضافة إلى عدة وظائف أخرى مثل تحديد الفولتات ومواصفات الكابل ومقويات Repeaters

Data Link Layer : وهي الطبقة الثانية من OSI Layer تؤمن هذه الطبقة اتصال بين الأجهزة الموجودة على نفس الشبكة مستعينتا بالعنوان الفيزيائي للجهاز Mac Address ومن أهم وظائفها إيجاد أفضل وقت لإرسال الداتا والأعلام عن الأخطاء في حال حدوثها وهي تقسم إلى طبقتان فرعيتان الأولى Logical Link Control والثانية Media Access Control وهي تعد الطبقة التي يعمل عليها السويتش

Network Layer : وهي الطبقة الثالثة من OSI Layer وهي مسؤولة عن عنوانة الداتا وتجهيزها بالعنوان اللازمة بالإضافة إلى إيجاد أفضل مسار يمكن الوصول إليه بين المصدر والهدف وهي الطبقة التي يعمل عليها الراوتر

Transport Layer : وهي الطبقة الرابعة من OSI Layer وهي مسؤولة عن نقل البيانات والتأكد من وصولها بشكل سليم إلى الهدف ويتم ذلك من خلال استخدام مجموعة من البروتوكولات مثل ال TCP & UDP

Session Layer : وهي الطبقة الخامسة من OSI Layer تقوم هذه الطبقة بتحديد آلية الفتح والأغلاق بين الطرفين المتصلين بالإضافة إلى إدارة الاتصال بينهم

Presentation Layer : وهي الطبقة السادسة من OSI Layer وهي مسؤولة عن أعداد البيانات من خلال ترجمتها وتنسيقها ضمن معايير متفق عليها بالإضافة إلى ضغط وتشفير البيانات أو العكس

Application Layer : وهي الطبقة الأخيرة من OSI Layer وهي طبقة البرامج والتطبيقات التي تستخدم الشبكة وهي واجهة المستخدم للاتصال مع الشبكة وتشمل هذه الطبقة برامج وتطبيقات مثل برامج تصفح الأنترنت أو البريد الإلكتروني أو برامج نقل البيانات عبر الشبكة والكثير

مشاكل وحلول

سوف يتم تخصيص هذا القسم لعرض المشاكل التي قد تواجهك في الشبكة بالإضافة إلى طريقة حل المشكلة كما أرحب أيضا بأرسال مشاكلكم على بريد المجلة magazine@networkset.net للنظر فيها وتقديم أفضل الحلول لها .

سؤال: ما أهمية الـ Process-id في الـ OSPF ؟

للإجابة على هذا السؤال يجب أن نعرف أن الـ Procsee ID في الـ OSPF لا يتعلق بباقي الروترات وهو خاص بي الروتر لوحده وبمعنى آخر local to the router only أي أن روتران في نفس الأريا سوف يعملان حتى لو كان الـ Process id مختلف وهي تفيد في حال كان الروتر يملك multiple OSPF على نفس الروتر ونريد أن تكون كل عملية منعزلة عن الأخرى لذا نلجأ لأعطاء كل عملية منها ايدي مختلف عن الآخر والرانج الخاص بها يبدأ من واحد وينتهي بي 65535 والأمر يكتب على الشكل التالي Router OSPF 3 وطبعا الأمر مختلف في EIGRP لان الـ Process id هناك يجب ان يكون موحد على كل الروترات

سؤال: ماهو local port and remote port وما هو الفرق بينهم ؟

جواب: عند دراستك الـ OSI Layer وخصوصا في الطبقة الرابعة Transport Layer سوف تجد جوابك وبشكل عام هذه الطبقة كما هو معروف عنها أنها تقوم بتحديد نوع البروتوكول المستخدم TCP أو UDP بالإضافة إلى وظائف أخرى وطريقة الاختيار ترجع إلى نوعية التطبيق الذي تستخدمه فإذا كنت تستخدم تطبيق الـ HTTP وتريد ان تتصفح أحد المواقع فأنت تستخدم أحد البورتات العشوائية الموجودة عندك للاتصال مع البورت 80 وكما هو معروف ان عدد البورتات هو 65536 أول 1023 بورت محجوز لخدمات معينة مثل http,ftp,dns,dhcp الخ وباقي البورتات تعتبر للاستخدام العام فمنها من يستخدم لبعض البرامج مثل الماسنجرات أو اي برنامج يتطلب استخدامه الأنترنت لذا الفكرة ببساطة هي ان الـ local Port هو الـ Source Port الذي يتم كتابته في الهيدر الخاص بي الـ TCP او الـ UDP بينما الـ Remote Port هو الـ Destination Port فعندما تتصفح الأنترنت أو اردت طلب صفحة معينة فأنت تضع في الهيدر الخاص بي الـ TCP رقم بورت عشوائي وليكن 1025 وهو يمثل السورس بورت أو لوكال بورت بينما تضع البورت 80 ليكون هو الـ ريموت بورت أو الـ Destination Port والسبب يعود كون التطبيق الخاص بي الـ HTTP في السيرفر الي يحوي الموقع يكون مفتوح على البورت 80 ويتسمع على انواع الترافيك الذي يصل اليه وعندما يصل الطلب سوف ينظر الى الهيدر ليكتشف أن هذا الطلب قادم لخدمة الـ HTTP فيأخذ الطلب ويضع المطلوب بداخله ويعيد ارساله لكن هذا المرة سوف يرد بان يضع اللوكال بورت رقم عشوائي بينما الـ ريموت بورت سوف يكون 80

مشكلة: انا عندي فى الشغل روتر سيسكو 1841 وأريد أن طريقة أقوم بوصل الأنترنت مع الروتر من خلال مودم DSL فما هي الأعدادات اللازمة للقيام بهذا الموضوع ؟

الحل: كل ما عليك ان تقوم به على الروتر هو الـ default route للشبكة من خلال الأمر ip route 0.0.0.0 0.0.0.0 192.168.1.1 ويكون أيبى المودم وبعدها اتجه إلى السويتش وقم بكتابة الأمر التالي ip default-gateway 172.16.1.1 والايبي طبعا خاص بالمنفذ الموجود على الروتر والممتل مع السويتش (الخطوة الثانية تقوم بعملها في حال كان السويتش عندك قابل للأعداد) ملاحظة صغيرة تقنية الـ PAT مفعلة على الروتر By Default